ENTRUST

POLITIQUE MONDIALE DE PROTECTION DES DONNÉES PERSONNELLES

Version du document	1.6
Date	5 septembre 2023

Sommaire

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 contractuelles applicables, ainsi qu'aux exigences en matière de certification et d'audit. La présente politique s'applique à tous les traitements de données personnelles effectués directement par Entrust et indirectement par des tiers qui traitent des données personnelles en notre nom.

3. Définitions

« Contrôleur de données » désigne l'entité qui détermine la finalité et les moyens du traitement des données personnelles. Synonyme du terme « Contrôleur d'informations personnelles identifiables » dans la norme ISO 27701.

« Processeur de données » désigne l'entité qui traite les données personnelles pour le compte du contrôleur de données. Synonyme du terme « Processeur d'informations personnelles identifiables » dans la norme ISO 27701.

« Analyse d'impact relative à la protection des données » désigne une analyse documentée réalisée par un contrôleur ou un processeur de données, qui évalue les risques pour le respect de la vie privée lorsque le traitement est susceptible de compromettre les droits et les libertés de la personne concernée.

« **Lois sur la protection des données** » désigne toutes les lois et réglementations en matière de protection des données et de respect de la vie privée applicables à Entrust, y compris, mais sans s'y limiter, le Règlement général sur la protection des données (RGPD) de l'UE, le Règlement général sur la protection des données (RGPD) du Royaume-Uni, la Loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE) et les lois des États américains sur le respect de la vie privée, qui peuvent être modifiés ou remplacés.

« Personne concernée » désigne la personne ou le foyer identifié ou identifiable auquel se rapportent les données personnelles. Synonyme du terme « Porteur d'informations personnelles identifiables » dans la norme ISO 27701.

« Analyse d'impact relative au transfert de données » fait référence à une analyse documentée réalisée par un contrôleur ou un processeur de données portant sur l'impact et les

implications en matière de sécurité d'un transfert de données personnelles vers un pays situé en dehors de l'Espace économique européen (regroupant les pays couverts par le RGPD) qui n'a pas fait l'objet d'une décision d'adéquation de la part de la Commission européenne.

« Analyse d'impact relative à l'intérêt légitime » désigne une analyse documentée réalisée par un contrôleur ou un processeur de données afin de déterminer si l'intérêt légitime peut être utilisé comme base juridique pour le traitement des données personnelles. Cette analyse comprend un test à trois volets permettant d'évaluer si le traitement des données personnelles répond à 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 » est synonyme des termes « informations personnelles identifiables », « informations personnelles » ou équivalents, tels que définis par les lois sur la protection des données.

« Incident relatif aux données personnelles » est synonyme des termes « incident de sécurité », « atteinte à la sécurité », « atteinte aux données personnelles » ou équivalents, tels que définis dans les lois sur la protection des données. Ces termes désignent toute situation dans laquelle Entrust apprend que des données personnelles ont été ou sont susceptibles d'avoir été consultées, divulguées, modifiées, perdues, détruites ou utilisées par des personnes non autorisées, d'une manière non autorisée.

« Traitement » désigne toute opération ou tout ensemble d'opérations effectuées sur des données personnelles, que ce soit par des moyens automatiques tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, diffusion ou toute autre mise à disposition, l'alignement 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 » désigne un sous-ensemble des données personnelles et fait référence aux informations sur une personne concernée qui, si elles sont perdues, compromises, consultées ou divulguées de manière inappropriée, pourraient entraîner un préjudice, un embarras, un désagrément ou une injustice pour la personne concernée et qui sont donc soumises à une protection accrue.

« Données de catégorie spéciale » désigne un sous-ensemble des données personnelles et fait référence aux informations sur l'origine raciale ou ethnique d'un individu, sa vie sexuelle ou son orientation sexuelle, ses opinions politiques, ses croyances religieuses ou philosophiques, son appartenance à des organisations syndicales, ses données génétiques ou biométriques (couleur des yeux, couleur des cheveux, taille, poids, par exemple), ses antécédents médicaux et son casier judiciaire.

4. Principes fondamentaux du traitement des données personnelles

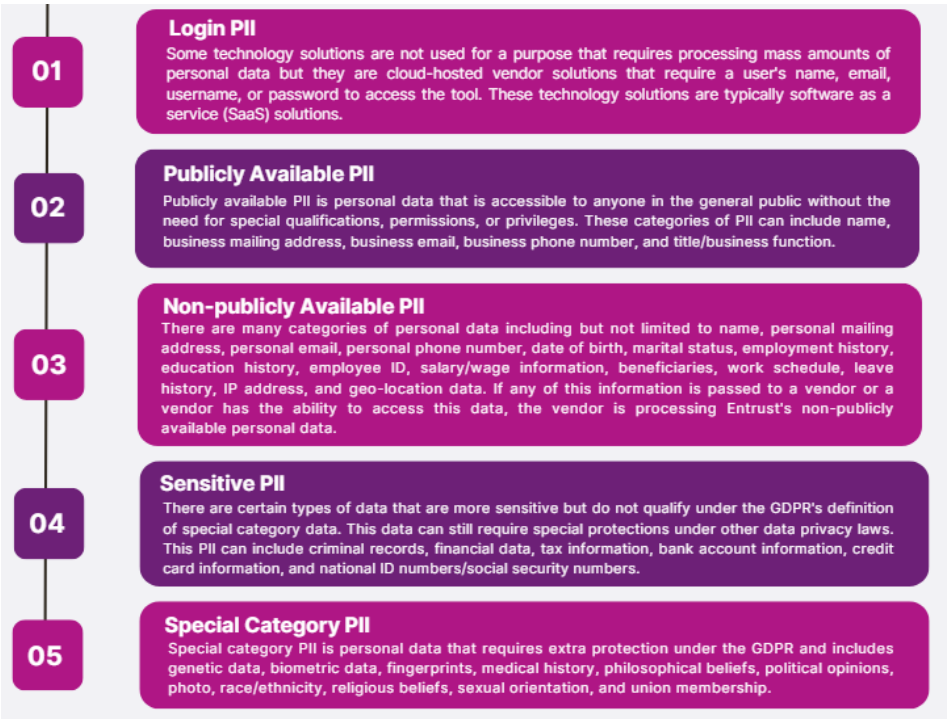
Entrust respecte les principes fondamentaux suivants lors du traitement des données personnelles :

- **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** : nous tenons nos systèmes à jour, nous fournissons des mécanismes permettant de mettre à jour ou de supprimer les données personnelles inexactes et nous ne conservons pas les données personnelles plus longtemps qu'il n'est nécessaire pour atteindre la finalité légitime du traitement.
- **Confidentialité et intégrité** : nous veillons à ce que les données personnelles soient sécurisées et protégées pendant leur traitement et nous réagissons rapidement et de manière appropriée aux éventuels incidents de sécurité et violations de données, y compris en fournissant des notifications opportunes, le cas échéant.
- **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 sommes tous responsables du traitement et de la protection appropriés des données personnelles et comprenons que tout manquement à cet égard risque non seulement d'entamer la confiance des clients dans Entrust, mais aussi d'entraîner des amendes et des pénalités importantes pour la Société.

5. Classification des données

Entrust tient un registre central de ses activités de traitement. Toutes les données personnelles sont classées dans l'une des catégories suivantes :



6. Conformité à la loi et adéquation

6.1 Fondements juridiques du traitement des données personnelles

La Société ne traite les données personnelles que dans la mesure où la loi l'autorise et après en avoir informé la personne concernée. Entrust s'appuie principalement sur les bases juridiques suivantes pour le traitement :

- exécution d'un contrat ;
- respect des obligations légales, y compris, mais sans s'y limiter, les demandes légitimes de la police ;
- intérêt légitime, sauf lorsque les intérêts ou les droits et libertés fondamentaux de la personne concernée l'emportent sur cet intérêt ;
- consentement.

Lorsque le consentement est le fondement juridique du traitement (par exemple, à des fins de marketing), Entrust s'assure qu'il 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 quelque raison que ce soit.

6.2 Analyses relatives au respect de la vie privée

6.2.1 Analyse relative au respect de la vie privée dès la conception

Entrust évalue le traitement des données personnelles par rapport aux principes fondamentaux dans le cadre de la conception et du développement d'offres de produits nouvelles ou substantiellement modifiées et lors de l'intégration de solutions de fournisseur hébergées dans le cloud, y compris lorsqu'elles font partie d'applications logicielles sous licence d'une tierce partie. L'analyse relative au respect de la vie privée dès la conception est intégrée dans les processus de développement et d'intégration des fournisseurs d'Entrust et contrôlée par les équipes chargées de la conformité et de la sécurité des informations. Le développement ne peut pas se faire sans approbation.

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

Lorsque le traitement des données personnelles envisagé présente un risque élevé pour les droits et libertés d'une personne, Entrust réalise une DPIA formelle pour documenter et évaluer l'objectif du traitement, la manière dont Entrust se conformera aux lois sur la protection des données en vigueur et la manière dont la Société atténuera les risques potentiels pour les droits de la personne concernée.

6.2.3 Analyse d'impact relative au transfert de données (DTIA)

Lorsqu'Entrust envisage de transférer des données personnelles vers un pays situé en dehors de l'Espace économique européen (EEE) qui ne bénéficie pas d'une décision d'adéquation de la Commission européenne, Entrust réalise une DTIA formelle pour analyser l'impact et les implications du transfert en matière de sécurité, en particulier lorsque les lois du pays destinataire peuvent autoriser son gouvernement à accéder aux données personnelles transférées.

6.2.4 Analyse d'impact relative à l'intérêt légitime (LIIA)

Lorsqu'Entrust utilise l'intérêt légitime comme fondement juridique du traitement des données personnelles, la Société réalise une LIIA formelle pour documenter et évaluer l'intérêt légitime, déterminer si le traitement est nécessaire et évaluer si les droits de la personne concernée l'emportent sur l'intérêt légitime.

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

En tant que contrôleur de données, Entrust traite des informations personnelles sensibles au nom de ses collaborateurs dans divers systèmes d'entreprise, ainsi que certaines données de catégorie spéciale, sur la base du volontariat et dans la mesure où la législation locale l'autorise. Des contrôles appropriés sont mis en place et décrits dans les DPIA applicables et la norme de contrôle d'accès aux données sensibles et de catégorie spéciale. Une formation renforcée au respect de la vie privée est obligatoire pour les collègues qui traitent les données sensibles et de catégorie spéciale.

6.3 Protections contractuelles

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

Les entreprises du groupe Entrust (c'est-à-dire toutes les personnes morales et les filiales) s'engagent à respecter l'accord intra-groupe sur le transfert de données, qui garantit la mise en place de mesures de protection appropriées pour le transfert de données personnelles hors de l'EEE, mais au sein du groupe Entrust, vers un pays qui ne bénéficie pas d'une décision d'adéquation de la part de la Commission européenne.

6.3.2 Accord de traitement des données (DPA)

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 garantissant que le tiers (par exemple, le vendeur, le fournisseur ou le partenaire de distribution) a mis en place des mesures techniques et organisationnelles appropriées pour se conformer aux lois en vigueur sur la protection des données. Entrust prend des engagements équivalents lorsqu'il agit en tant que processeur de données dans le cadre d'un DPA standard avec le client.

6.3.3 Dispositions générales relatives au respect de la vie privée.

Le langage contractuel relatif au respect 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 standard d'Entrust.

7. Précision et conservation

7.1 Gestion des dossiers

Le programme mondial de gestion des dossiers garantit qu'une période de conservation est définie formellement pour le traitement des données personnelles afin de s'assurer qu'elles ne sont détenues que pendant la durée nécessaire et qu'elles sont effacées, détruites ou rendues anonymes à la fin de la période de conservation définie. La politique mondiale de gestion des dossiers définit 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 de chaque type de dossier géré par la Société.

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 la Société. Les services informatiques et les fournisseurs concernés (pour les applications hébergées dans le cloud et non gérées par les services informatiques) reçoivent des consignes standard relatives au 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 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 personnelles ne doivent pas être copiées, sauf si cela est nécessaire pour atteindre l'objectif spécifié du traitement, et toutes les copies effectuées doivent porter les mêmes marques de confidentialité ou de propriété que les originaux.
- Les documents papier doivent être déchiquetés et éliminés en toute sécurité lorsqu'il n'est plus nécessaire de les conserver ; ils ne peuvent être éliminés d'aucune autre manière.
- Les données personnelles au format électronique doivent être supprimées ou rendues anonymes lorsqu'elles ne sont plus utilisées.
- Le service informatique est chargé de détruire ou d'effacer les équipements électroniques contenant des données personnelles (par exemple, les ordinateurs portables, les ordinateurs de bureau, les appareils mobiles appartenant à l'entreprise et les données professionnelles sur les appareils BYOD) conformément aux politiques et aux normes en vigueur relatives à la sécurité des informations.

8. Confidentialité et intégrité

8.1 Sécurité des informations

Lorsque la Société traite des données personnelles, elle prend des mesures appropriées pour s'assurer que ces données soient sécurisées et protégées contre le traitement non autorisé ou illégal, la perte accidentelle, la destruction ou les dommages. Pour appliquer ces mesures, Entrust :

- chiffre les données personnelles au repos et en transit lorsque la loi ou le contrat l'exige et dans la mesure où cela est commercialement réalisable ;
- garantit la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et des services utilisés pour traiter les données personnelles grâce à des plans formalisés de reprise des activités et de récupération après sinistre qui sont régulièrement testés ou mis à l'épreuve ;

- 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 et mettre en œuvre des mesures techniques et organisationnelles adéquates 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 (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 environnements de test doivent être supprimées immédiatement une fois les tests terminés. La 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) ;

- cyber-attaque (par exemple, ouverture d'une pièce jointe à un e-mail provenant d'un tiers inconnu contenant un rançongiciel ou d'autres logiciels malveillants) ;
- autoriser l'utilisation/l'accès non autorisé (par exemple, permettre à un tiers non autorisé d'accéder aux zones sécurisées des bureaux ou des systèmes d'Entrust) ;
- destruction physique et perte (par exemple, en cas d'incendie ou d'inondation) ;
- informations fournies par Entrust à un tiers par le biais d'une tromperie (attaque par hameçonnage, par exemple).

Les situations suivantes peuvent indiquer qu'un incident relatif aux données personnelles s'est produit :

- nombre de connexions inhabituel et/ou activité excessive du système en ce qui concerne les comptes d'utilisateurs actifs ;
- activité d'accès à distance inhabituelle ;
- présence de faux réseaux sans fil (Wi-Fi) visibles ou accessibles depuis l'environnement de travail d'Entrust ;
- défaillance matérielle ;
- enregistreurs de frappe matériels ou logiciels connectés ou installés sur les systèmes Entrust.

Les collaborateurs qui ont connaissance d'un incident lié aux données personnelles ou qui ont des raisons de soupçonner qu'un tel incident s'est produit ou est sur le point de se produire, doivent immédiatement contacter le centre des opérations de sécurité d'Entrust à l'adresse suivante : SOC@entrust.com.

8.4 Réponse aux incidents liés aux données personnelles

En cas d'incident réel ou imminent concernant des données personnelles, Entrust met en œuvre les procédures d'intervention et de gestion des incidents établies par l'équipe de sécurité des informations afin de minimiser l'impact de l'incident et d'aviser les organismes de réglementation, les personnes concernées et/ou d'autres parties, conformément à ses obligations légales et/ou contractuelles. Une intervention comprend généralement les mesures suivantes :

- enquêter sur l'incident pour déterminer la nature, la cause et l'étendue des dommages ou préjudices pouvant en résulter ;
- 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 (autorités nationales de protection des données, personnes concernées ou parties contractuelles, par exemple) et déclencher ces notifications rapidement ;
- enregistrer les informations relatives à l'incident lié aux données personnelles et les mesures prises pour y remédier, y compris les décisions de notifier ou non les autorités de régulation ou les parties concernées.

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. Ces avis fournissent des informations sur :

- les types de données personnelles traitées par Entrust ;
- l'objectif et le fondement juridique du traitement ;
- les tiers utilisés pour le traitement, le cas échéant ;
- le lieu et la durée du traitement ;
- tout transfert transfrontalier de données personnelles ;
- la durée du traitement ;
- les droits de la personne concernée ;
- des informations sur les processus de prise de décision basés sur l'intelligence artificielle/automatisés.

9.2 Formation

Entrust propose à ses collaborateurs une formation annuelle obligatoire sur les responsabilités en matière de protection des données. Cette formation, qui fournit une présentation de la confidentialité des données, a lieu au moment de l'intégration et une fois par an par la suite. En plus de cette formation destinée à l'ensemble des collaborateurs, Entrust exige que les collaborateurs qui traitent des données sensibles et de catégorie spéciale suivent chaque année la formation étendue à la confidentialité des données et que les collaborateurs impliqués dans le développement et la conception de produits et de services logiciels suivent la formation à la protection de la vie privée dès la conception. Entrust continue à développer et à déployer d'autres formations sur la confidentialité spécifiques aux fonctions, en fonction des besoins.

9.3 Droits de la personne concernée

Lorsqu'Entrust traite des données personnelles, les personnes concernées ont 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 informations sur les données personnelles détenues les concernant ;
- faire rectifier les données personnelles inexactes les concernant et compléter les données personnelles incomplètes ;
- s'opposer au traitement de ses données personnelles par Entrust lorsque la Société agit dans le cadre de ses propres intérêts légitimes. Entrust peut continuer à traiter les

données personnelles nonobstant 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 motifs juridiques ;
- demander à Entrust de détruire les données personnelles les concernant. 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 juridique pour qu'Entrust continue le traitement ;
- demander à Entrust de limiter le traitement de leurs données personnelles au stockage dans certaines circonstances.

Entrust évalue les droits d'une personne concernée en vertu des lois sur la protection des données au cas par cas et suit la procédure applicable aux demandes des personnes concernées pour déterminer comment répondre à une demande. En général, Entrust utilise les droits d'une personne concernée en vertu du RGPD de l'UE comme référence pour répondre à toutes les demandes et applique les droits supplémentaires accordés par les lois en matière de protection des données à la personne concernée, dans la mesure où ceux-ci 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 qui souhaitent demander des informations sur les données personnelles qu'Entrust détient à leur sujet doivent le faire en soumettant une demande de personne concernée (DSR). Si les collaborateurs reçoivent une demande directement (verbalement ou par écrit), celle-ci doit être immédiatement transmise à 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 Conseil européen de la protection des données se trouve ici. Le Bureau du commissaire à l'information (ICO) du Royaume-Uni se trouve ici. Le Bureau du Commissaire à la protection de la vie privée du Canada se trouve ici.

10. Conformité

Tous les collaborateurs et travailleurs occasionnels doivent 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 pourront entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. La présente politique peut être mise à jour ou modifiée à tout moment.

11. Exceptions

Il n'existe aucune exception à la présente politique.

12. Propriété et révision

La présente politique est détenue par le Directeur des affaires juridiques et de la conformité et doit être révisée chaque année.

12.1 Coordonnées de contact

Les questions concernant la présente politique ou le traitement des données personnelles par Entrust peuvent être adressées à privacy@entrust.com.