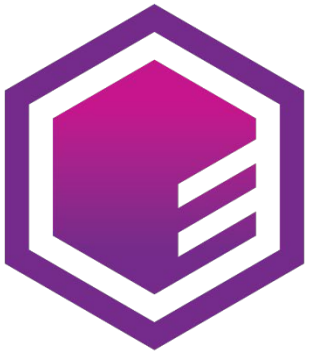

ENTRUST

POLITIQUE GLOBALE DE PROTECTION DES DONNÉES PERSONNELLES

Version du document	1.4
Date	10-déc-2021

Sommaire

1. Introduction

En tant qu'entreprise et employeur, il est nécessaire pour Entrust Corporation et ses filiales et sociétés affiliées (collectivement, « Entrust » ou la « Société ») de collecter, stocker et traiter des données personnelles sur nos employés, travailleurs intérimaires, clients, fournisseurs et autres. des tiers avec lesquels nous nous engageons pour fournir des produits ou des services en notre nom.

Avec l'introduction du Règlement général européen sur la protection des données (« RGPD ») le 25 mai 2018 et d'autres lois applicables régissant la protection des données, nous sommes soumis à des exigences renforcées concernant la manière dont nous collectons, utilisons et stockons les données personnelles.

2. Objet

Le but de cette politique est de nous aider tous à respecter nos obligations légales et de permettre aux personnes sur lesquelles nous détenons des données personnelles d'avoir confiance en nous. Cette politique s'applique à tous les employés d'Entrust, aux travailleurs intérimaires et aux tiers qui traitent des données au nom d'Entrust. Sauf indication contraire, cette politique s'applique dans tous les pays dans lesquels Entrust exerce ses activités et/ou exerce ses activités.

3. Exigences de la politique

3.1 Définitions

« Contrôleur des données » ou **« Contrôleur des informations personnellement identifiables (contrôleur PII) »** désigne l'entité qui détermine la finalité et les moyens du traitement des données personnelles.

"Processeur de données" ou **« Processeur d'informations personnellement identifiables (processeur PII) »** désigne l'entité qui traite les données personnelles au nom du contrôleur.

« Lois sur la protection des données » désigne toutes les lois et réglementations applicables en matière de protection des données et de confidentialité des données, 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 du Royaume-Uni (RGPD), la Loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE) et le California Consumer Privacy Act (CCPA).

« Personne concernée » ou **« Principal d'informations personnellement identifiables (PII principal) »** désigne la personne ou le foyer identifié ou identifiable auquel les données personnelles se rapportent.

« Utilisateur de données » est un terme utilisé pour décrire tout employé, consultant, entrepreneur indépendant, stagiaire, travailleur temporaire ou tiers agissant au nom d'Entrust (y

compris les sous-traitants) dont le travail implique le traitement de données personnelles pour Entrust.

"Données personnelles" aura le sens attribué à « informations personnellement identifiables », « informations personnelles », « données personnelles » ou à des termes équivalents tels que ces termes sont définis dans les lois sur la protection des données.

« Incident de données personnelles » aura le sens attribué par les lois sur la protection des données aux termes « incident de sécurité », « violation de la sécurité » ou « violation des données personnelles » et comprendra toute situation dans laquelle le Vendeur apprend que des Données personnelles ont été ou sont susceptibles d'avoir été consultées, divulgués, modifiés, perdus, détruits ou utilisés par des personnes non autorisées, d'une manière non autorisée.

"Traitement" désigne toute opération ou ensemble d'opérations qui est effectué sur les Données personnelles, que ce soit par des moyens automatiques ou non, tels que la collecte, l'enregistrement, la structuration de l'organisation, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la divulgation par transmission, diffusion ou autre disponibles, alignement ou combinaison, restriction, effacement ou destruction. Le traitement comprend également le transfert ou la divulgation de données personnelles à des tiers.

« Données de catégorie spéciale » ou **« Informations personnelles de catégorie spéciale »** est un sous-ensemble de données personnelles et fait référence à des informations sur la race ou l'origine ethnique d'un individu, sa vie sexuelle ou son orientation sexuelle, ses opinions politiques, ses convictions religieuses ou philosophiques, son appartenance à un syndicat, ses données génétiques, ses données biométriques (couleur des yeux, couleur des cheveux, taille, poids), antécédents médicaux ou condamnations pénales et infractions ou mesures de sécurité connexes.

3.2 Responsabilité première

Selon les circonstances, Entrust peut agir à titre de contrôleur de données ou de sous-traitant. En tant que contrôleur de données, Entrust est chargé d'établir des pratiques et des politiques conformes aux lois sur la protection des données. Il est tout aussi important qu'Entrust soit en mesure de démontrer la conformité à ces lois. La Société le fait en :

- Mettre en œuvre des politiques qui permettent à la Société de se conformer aux lois sur la protection des données telles que cette politique, les politiques concernant la conservation des documents et la sécurité des données, et les déclarations de confidentialité d'Entrust ;
- Communiquer et former les employés, les travailleurs intérimaires et les tiers agissant au nom d'Entrust sur les exigences en matière de protection des données ;
- Enquêter sur les cas de non-respect des politiques de protection des données d'Entrust et prendre les mesures correctives et/ou disciplinaires appropriées ;

- Enquêter, corriger et, dans certains cas, fournir une notification d'un incident de données personnelles ;
- Réaliser des évaluations d'impact du traitement des données, le cas échéant, pour de nouveaux types d'activités de traitement ;
- Entreprendre des audits internes périodiques des politiques et procédures de protection des données d'Entrust ; et
- Tenir compte de la protection des données dès le début de la conception d'un nouveau produit.

3.3 Traitement des données personnelles

Toutes les données personnelles que la Société traite ou qui sont traitées pour le compte d'Entrust doivent :

- être traitées loyalement, licitement et de manière transparente ;
- être traitées uniquement pour des finalités déterminées, explicites et légitimes ;
- Être pertinent et limité à ce qui est nécessaire aux fins légitimes pour lesquelles les données sont traitées ;
- Être précis et tenu à jour en veillant, dans la mesure du possible, à ce que les données personnelles inexactes soient effacées ou rectifiées sans délai ;
- Ne pas être conservées plus longtemps que nécessaire pour atteindre la ou les finalités pour lesquelles les données ont été collectées ; et
- Être traitées de manière à garantir une sécurité appropriée des données personnelles, y compris la protection contre le traitement non autorisé ou illégal, la perte accidentelle, la destruction ou les dommages.

3.4 Traitement des données de catégorie sensible et spéciale

Entrust traite les informations sensibles pour le compte de ses collègues sur divers systèmes d'entreprise et des données de catégories spéciales limitées dans Workday. Des contrôles appropriés sont en place et décrits dans les DPIA sur les données de catégorie spéciale, les avantages sociaux et la paie et la norme de contrôle d'accès pour les données de catégorie sensible et spéciale disponibles sur le site de conformité d'Entrust.

3.5 Motifs juridiques du traitement des données personnelles

La Société ne peut traiter des données personnelles que si elle est autorisée à le faire en vertu des lois sur la protection des données. Les motifs sur lesquels Entrust s'appuie pour traiter les données personnelles sont les suivants :

Lorsque le traitement est nécessaire :

- Pour l'exécution d'un contrat auquel la personne concernée est partie, ou pour prendre des mesures à la demande de la personne concernée avant de conclure un contrat ;

- Pour se conformer à une obligation légale à laquelle Entrust est soumis, y compris, mais sans s'y limiter, les demandes légales des autorités chargées de l'application de la loi ; et/ou
- Pour poursuivre les intérêts légitimes d'Entrust, sauf lorsque ces intérêts sont outrepassés par les intérêts ou les libertés et droits fondamentaux de la Personne concernée.

En plus de ces motifs, Entrust peut également traiter des données personnelles lorsque la personne concernée a donné son consentement au traitement pour une ou plusieurs finalités déterminées, à condition que le consentement soit donné librement, spécifique, éclairé et qu'il indique sans ambiguïté les souhaits de la personne concernée. Lorsqu'Entrust utilise le consentement comme motif de traitement, une personne concernée a le droit de retirer son consentement à tout moment et pour quelque raison que ce soit.

Entrust peut, à l'occasion, également avoir besoin de traiter des catégories spéciales de données personnelles pour les clients, les employés ou les travailleurs intérimaires (par exemple, lorsque des pratiques d'emploi sûres l'exigent). Lorsqu'Entrust traite ou utilise un tiers pour traiter en son nom des catégories particulières de données personnelles, Entrust s'assurera, le cas échéant, que les conditions suivantes sont remplies :

- La personne concernée a donné son consentement explicite au traitement de la catégorie spéciale de données à caractère personnel pour une ou plusieurs finalités spécifiées ;
- Le traitement est nécessaire à l'exécution d'obligations en vertu du droit du travail, du droit de la sécurité sociale ou de la protection sociale, ou d'une convention collective ;
- Le traitement est nécessaire à des fins de médecine préventive ou du travail, ou pour l'évaluation de la capacité de travail d'un employé ;
- Le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement ;
- Le traitement concerne des données personnelles qui ont été rendues publiques par la personne concernée ; et/ou
- Le traitement est nécessaire pour établir ou défendre des réclamations légales.

3.6 Gestion des enregistrements de données

Entrust conserve un enregistrement central des types de données personnelles que la Société collecte et des raisons pour lesquelles ces données sont collectées. Entrust ne traitera les données personnelles qu'aux fins spécifiques énoncées dans le fichier central ou à toute autre fin spécifiquement autorisée par les lois sur la protection des données. Entrust informera les personnes concernées de ces finalités lors de la première collecte des données ou, si cela n'est pas possible, dès que possible par la suite.

Entrust ne traitera les données personnelles que dans la mesure requise pour les finalités fournies à la personne concernée. Cela signifie qu'Entrust ne peut pas demander, ou enregistrer

dans ses systèmes, plus de données personnelles que nécessaire. La Société a mis en place des mesures techniques et organisationnelles appropriées pour garantir que les données personnelles qui ne sont plus nécessaires soient effacées ou détruites.

La Société utilise également des mesures raisonnables pour s'assurer que toutes les données personnelles détenues sont exactes et tenues à jour. Entrust vise à vérifier l'exactitude de toutes les données personnelles au moment de la collecte et à intervalles réguliers par la suite. La Société prendra toutes les mesures raisonnables pour effacer, détruire ou modifier les données inexactes ou obsolètes sans retard injustifié et, en tout état de cause, dans un délai d'un mois à compter de la demande d'une personne concernée (ou jusqu'à trois mois s'il existe des raisons spécifiques pourquoi un mois n'est pas possible).

Pour plus d'informations sur la gestion et la conservation des documents, consultez le site Politique mondiale de gestion des dossiers et le Calendrier de conservation des dossiers associé.

3.7 Effacement ou destruction des Données personnelles

Les dossiers papier contenant des données personnelles doivent être déchiquetés et éliminés en toute sécurité lorsqu'il n'est plus nécessaire de les conserver. *Les dossiers papier contenant des données personnelles ne peuvent être éliminés d'aucune autre manière.*

Lors de la suppression de données personnelles électroniques, toutes les mesures possibles doivent être prises pour mettre les données en question hors d'usage. Lorsqu'il est impossible de supprimer complètement les données personnelles, des mesures raisonnables doivent être prises pour garantir que les données sont supprimées dans toute la mesure du possible.

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 les appareils BYOD).

3.8 Sécurité de l'information

Lorsque la Société traite des données personnelles, elle prend des mesures raisonnables pour s'assurer que les données restent sécurisées et sont protégées contre le traitement non autorisé ou illégal, la perte accidentelle, la destruction ou les dommages. Entrust le fait en :

- Crypter les données personnelles lorsque cela est possible et approprié ;
- Assurer la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et services utilisés pour traiter les données personnelles ;
- Assurer le rétablissement de l'accès aux données personnelles en temps opportun en cas d'incident physique ou technique ; et
- Faciliter les tests, l'évaluation et l'évaluation de l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité des données.

En évaluant le niveau de sécurité approprié, Entrust prend en compte les risques associés au traitement, 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, ces parties le font sur la base d'instructions écrites, sont soumises à une obligation de confidentialité et sont tenues de mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité des données. Les données personnelles ne peuvent être partagées avec quiconque en dehors d'Entrust ou de tiers autorisés.

Les bureaux et armoires sont fermés à clé s'ils contiennent des données personnelles ou des informations confidentielles de quelque nature que ce soit. Les utilisateurs de données s'assurent que les moniteurs/écrans individuels ne montrent pas de données personnelles ou d'informations confidentielles aux passants et qu'ils se déconnectent ou verrouillent leurs ordinateurs/tablettes lorsqu'ils sont laissés sans surveillance.

3.9 Signaler un incident de données personnelles

Un incident de données personnelles peut se produire de plusieurs manières, notamment :

- 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 (par exemple, volé dans un véhicule ou à la maison) ;
- 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);
- Des circonstances imprévues telles qu'un incendie ou une inondation ; ou
- Lorsque des informations sont obtenues d'Entrust par un tiers par tromperie.

Les signes qu'un incident de données personnelles a pu se produire sont les suivants :

- Connexion inhabituelle et/ou activité excessive du système, en particulier en ce qui concerne les 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 ;
- Défaillance de l'équipement ; et
- Enregistreurs de frappe matériels ou logiciels connectés ou installés sur les systèmes Entrust.

Les collègues qui ont connaissance ou ont des raisons de soupçonner qu'un incident relatif aux données personnelles s'est produit ou est sur le point de se produire doivent immédiatement contacter le Centre des opérations de sécurité d'Entrust par courrier électronique à l'adresse SOC@entrust.com et le directeur de la conformité de privacy@entrust.com.

3.10 Plan de réponse aux incidents de données personnelles

En cas d'incident de données personnelles réel ou imminent, Entrust prend des mesures rapides pour minimiser l'impact de l'incident et signaler l'incident si la loi l'exige. Dans la plupart des cas, la réponse impliquera :

- 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 les autres parties (par exemple, les autorités nationales de protection des données, les personnes concernées) et effectuer ces notifications. S'il existe une obligation d'informer les autorités de protection des données, le signalement doit généralement avoir lieu dans les 72 heures suivant la prise de connaissance de l'incident par la Société, y compris l'un de ses employés ; et
- Enregistrer des informations sur l'incident de données personnelles et les mesures prises en réponse, y compris la documentation qui explique la décision de notifier ou de ne pas notifier.

3.11 Stockage et sauvegarde des données personnelles

Entrust utilise plusieurs emplacements de serveurs pour stocker et sauvegarder les données personnelles. Pour les emplacements de serveurs utilisés par des tiers avec lesquels Entrust s'engage pour traiter des données personnelles au nom de collègues et de clients, consultez les analyses d'incidence relatives à la protection des données pertinentes pour les données personnelles des collègues et la page du sous-traitant externe, ainsi que les avis de confidentialité des produits pour les données personnelles des clients. Ces documents sont tous disponibles en interne sur la page Conformité ou en externe sur le site Conformité légale sous les icônes de confidentialité des données. Pour obtenir une liste à jour des emplacements des serveurs de données d'entreprise, les collègues peuvent également contacter directement le service informatique.

3.12 Transferts internationaux de données et transferts à des tiers

En vertu du RGPD, Entrust peut transférer des données personnelles vers des pays situés en dehors de l'Espace économique européen (« EEE ») où il existe un niveau de protection adéquat dans ce pays ou lorsqu'Entrust a mis en place des mesures appropriées pour assurer la protection des données.

Les sociétés du groupe Entrust (c'est-à-dire toutes les entités corporatives et filiales) doivent conclure l'accord de transfert de données intra-groupe afin d'assurer des garanties appropriées pour le transfert de données personnelles en dehors de l'EEE, mais au sein du groupe Entrust.

Les entreprises extérieures au groupe Entrust qui traitent des données personnelles pour ou au nom d'Entrust, pour lesquelles Entrust agit en tant que responsable du traitement ou sous-traitant des données, doivent conclure un accord de traitement des données avec Entrust afin d'assurer des garanties appropriées pour le transfert de données personnelles en dehors du EEE. Cet accord contient des dispositions garantissant que le tiers dispose des mesures techniques et organisationnelles appropriées pour se conformer au RGPD et garantir la protection des droits des personnes concernées.

Les cas où Entrust transfère des données personnelles vers un pays en dehors de l'EEE peuvent inclure :

- La personne concernée a donné son consentement explicite au transfert proposé après qu'Entrust l'a informée des risques possibles associés à un tel transfert (par exemple, l'absence dans ce pays de garanties équivalentes) ;
- Le transfert est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou pour prendre des mesures à la demande de la personne concernée avant de conclure un contrat ;
- Le transfert est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement ; ou
- Le transfert est nécessaire à l'établissement ou à la défense d'une action en justice.

Pour chaque transfert de données en dehors de l'EEE, Entrust s'appuiera sur les clauses contractuelles types telles que définies par la Commission européenne (2001/497/CE, 2004/915/CE et 2010/87/UE).[1] Notez qu'un accord de transfert de données est également requis si vous transférez des données personnelles à l'extérieur du Canada.

3.13 Notifier les personnes concernées

Entrust est tenu de fournir des informations aux personnes concernées sur le traitement de leurs données personnelles. Ces informations sont contenues dans la déclaration de confidentialité Web de la société, qui est accessible au public à l'adresse www.entrust.com, la déclaration de confidentialité du demandeur d'emploi qui est accessible au public à l'adresse https://www.entrust.com/legal-compliance/data-privacy/job-applicant-privacy-statement, et la Déclaration de confidentialité des employés qui est disponible sur l'intranet d'Entrust. Ces déclarations fournissent des informations sur :

- Les types de données personnelles traitées par Entrust ;
- La finalité et la base juridique du traitement des données personnelles ;

[1] A compter du 27 décembre 2022, ces transferts s'effectueront selon les nouvelles clauses contractuelles types telles que décrites dans le Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil.

- Si les données personnelles seront divulguées à des tiers au cours du traitement ;
- Si les données personnelles seront transférées en dehors de l'EEE et du Canada et, le cas échéant, quelles garanties seront mises en place ;
- Combien de temps les données personnelles seront traitées ou, s'il n'est pas possible de déterminer, les critères que la Société utilisera pour déterminer la période de traitement ;
- Comment la personne concernée peut-elle obtenir une copie de ses données personnelles détenues par Entrust ;
- Les droits de la personne concernée, y compris la manière de déposer une plainte ;
- Si les données personnelles doivent être traitées afin de se conformer à une loi ou à un contrat, les conséquences possibles du défaut de la personne concernée de fournir les données ou de s'opposer au traitement ; et
- L'existence et les détails de tout processus décisionnel automatisé, le cas échéant.

Si Entrust reçoit des données personnelles concernant une personne concernée d'un tiers, la Société fournira également à la personne concernée des informations sur :

- Le type de données personnelles reçues du tiers ; et
- La source des données et si elles proviennent d'une source accessible au public (par exemple, un site Web accessible au public).

3.14 Évaluations d'impact sur la confidentialité dès la conception et la protection des données

Les lois sur la protection des données exigent qu'Entrust prenne en compte la protection des données pendant les étapes de développement d'une nouvelle offre de produits. Afin de satisfaire à cette obligation, Entrust doit prendre des mesures pour s'assurer que la protection des données fait partie du processus de conception et que la collecte de données personnelles est minimisée dans la mesure du possible.

Dans certaines circonstances (à savoir, lorsque le traitement entraînerait un risque élevé pour les droits et libertés d'une personne), Entrust peut être tenu de procéder à une évaluation formelle de l'impact sur la protection des données (DPIA) en ce qui concerne le traitement des données personnelles. Une telle évaluation implique de documenter les finalités pour lesquelles l'activité est réalisée, comment Entrust se conformera aux lois sur la protection des données et comment la Société atténuera les risques potentiels pour la vie privée des individus. Si vous pensez qu'une analyse d'impact sur la protection des données peut être nécessaire, contactez le directeur de la conformité à l'adresse privacy@entrust.com.

3.15 Droits des personnes concernées

Si Entrust traite des données personnelles, en vertu des lois sur la protection des données, la personne concernée peut avoir le droit de :

- Demander des informations sur les données personnelles détenues à leur égard ;

- Faire corriger les données personnelles inexactes les concernant et compléter les données personnelles incomplètes, sous réserve qu'Entrust détermine que les données sont, de fait, inexactes ou incomplètes ;
- S'opposer au traitement de leurs données personnelles par Entrust lorsque la Société le fait dans la poursuite 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 l'établissement ou la défense d'une action en justice ;
- 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 légitime pour qu'Entrust continue le traitement ;
- Demandez à Entrust de restreindre le traitement de leurs données personnelles au stockage. Cela ne peut être demandé que si l'exactitude des données personnelles a été contestée et reste non vérifiée ; Entrust n'a plus besoin des données personnelles, mais la personne concernée en a besoin pour établir ou défendre une action en justice ; la personne concernée s'est opposée au traitement des données personnelles ; et Entrust décide si ses intérêts légitimes l'emportent sur les intérêts de la personne concernée ou si le traitement est illégal.

Entrust évaluera les droits de la personne concernée en vertu de la législation applicable en matière de protection des données au cas par cas afin de déterminer comment répondre à une demande d'accès de la personne concernée. En général, Entrust utilisera les droits d'une personne concernée en vertu du RGPD de l'UE comme référence pour répondre aux demandes et appliquera les droits disponibles en vertu de la législation applicable en matière de confidentialité des données dans la mesure où ceux-ci sont plus favorables à la personne concernée. 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.

3.16 Droits d'accès de la personne concernée

Les personnes concernées qui souhaitent demander des informations sur les données personnelles que Entrust détient à leur sujet peuvent le faire en soumettant un Demande d'accès de la personne concernée (DSAR). Si des collègues reçoivent une demande directement (que ce soit verbalement ou par écrit), transmettez immédiatement les détails de la demande à privacy@entrust.com. Une liste plus complète des droits des personnes concernées par juridiction est disponible dans la Procédure de demande d'accès de la personne concernée sur le site Conformité.

3.17 Formation

Entrust offre à ses employés et travailleurs intérimaires un accès à une formation sur les responsabilités en matière de protection des données. Cette formation a lieu lors de l'intégration et à intervalles réguliers par la suite.

3.18 Autorités de surveillance

Les coordonnées des autorités de contrôle des données concernées varient selon le lieu. La liste des autorités du Comité européen de protection des données se trouve ici. Le Commissariat à la protection de la vie privée du Canada se trouve ici.

3.19 Délégué à la protection des données

Si vous avez des questions sur le système de gestion des renseignements personnels d'Entrust, veuillez communiquer avec :

Entrust Corporation.

Attention : Jenny Carmichael, directrice de la conformité

1187 Park Place

Shakopee, MN 55379

privacy@entrust.com

Le délégué à la protection des données de Entrust Deutschland GmbH est M. Niels Kill d'Althammer & Kill GmbH & Co. KG (kontakt-dsb@althammer-kill.de).

4. Conformité

Tous les employés 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 peuvent entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. La présente politique peut être mise à jour ou modifiée à tout moment.

5. Exceptions

Il n'existe aucune exception à la présente politique.

6. Propriété et révision

Cette politique est la propriété du Chief Legal and Compliance Officer. Cette politique doit être révisée annuellement. Les modifications apportées à ce document doivent être conformes à la norme de contrôle des documents et des enregistrements du système de gestion de la sécurité de l'information (SGSI).

6.1 Coordonnées

Les questions concernant cette politique ou les plaintes concernant le traitement des données personnelles doivent être adressées au directeur de la conformité à l'adresse privacy@entrust.com.

6.2 Propriétés du document et historique des révisions

Propriétés du document	
Propriété	**Description**
Circulation	Usage interne et externe
Classification	Public
Propriétaire du document	Lisa Tibbits, chef des affaires juridiques et de la conformité
Prochaine révision prévue	2022

Approbations des documents		
Nom de l'approbateur	**Fonction**	**Date**
Lisa Tibbits	Chef des affaires juridiques et de la conformité	3-Mar-2019
Conseil de gouvernance des politiques	S/O	3-août-2021
Conseil de gouvernance des politiques	S/O	16-déc-2021

Historique des révisions			
Version	**Date**	**Description des modifications**	**Révisé par**
1.0	19-Avr-2019	Version initiale	Anjali Doherty, Sr. Atty corporatif ; Jenny Carmichael, directrice de la conformité
1.1	19-Avr-2020	Mises à jour annuelles	Anjali Doherty, Sr. Atty corporatif ; Jenny Carmichael, directrice de la conformité
1.2	10-Sept-2020	Mis à jour dans un nouveau modèle de politique	Aileen Havel, spécialiste principale de la conformité
1.3	06-juil-2021	Révisions annuelles ; section ajoutée concernant l'accès aux données de catégorie spéciale	Aileen Havel, avocate d'entreprise associée ; Lee Jones, spécialiste principal de l'assurance de la conformité

1.4	10-déc-2021	Mises à jour pour se conformer aux contrôles ISO 27701 et aux recommandations d'évaluation des risques externes	Jenny Carmichael, directrice de la conformité