ENTRUST

# POLITIQUE GLOBALE DE PROTECTION DES DONNÉES PERSONNELLES

| | |
|---|---|
| Version du document | 1.5 |
| Date | 17 janvier 2023 |

**Sommaire**

## 1. Introduction

En tant qu'entreprise et employeur, il est nécessaire qu'Entrust Corporation et ses filiales et sociétés affiliées (collectivement, « Entrust » ou la « Société ) recueillent, stockent et traitent les données personnelles de nos employés, travailleurs externes, clients, fournisseurs et autres tiers avec lesquels nous nous engageons à fournir des produits ou services en notre nom.

En tant qu'entreprise mondiale, Entrust est soumise à des exigences accrues concernant la manière dont nous collectons, utilisons et stockons les données personnelles.

## 2. Objectif

Cette politique a pour objectif de nous aider tous à nous conformer à nos obligations légales et de permettre aux personnes pour lesquelles nous détenons des données personnelles d'avoir confiance en nous. Cette politique s'applique à tous les employés d'Entrust, aux employés externes 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 politiques

### 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 pour le compte du contrôleur.

« **Les lois sur la protection des données** » font référence à toutes les lois et réglementations applicables en matière de protection des données et de confidentialité des données, y compris, mais sans s'y limiter, à la loi EU General Data Protection Regulation (EGPD), UK General Data Protection Regulation (RGPD RU), Personal Information Protection and Electronic Documents Act (PIPEDA) du Canada, California Consumer Privacy Act, Colorado Privacy Act (CPA), Virginia Consumer Data Protection Act (VCDPA), Utah Consumer Privacy Act (UCPA) et Connecticut Data Privacy Act (CTDPA) (dans chaque cas, telles qu'elles peuvent être modifiées, supplantées ou remplacées)

**« Personne concernée »** ou **« Informations personnellement identifiables de la personne concernée (PII de la personne concernée) »** signifie la personne ou le ménage identifié(e) ou identifiable auquel les données personnelles se rapportent.

**« Données utilisateur »** 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.

**Les « Données Personnelles »** ont la signification attribuée aux termes « Informations personnellement identifiables », « Informations personnelles », « données personnelles » ou des termes équivalents tels que définis par les Lois sur la Protection des Données.

**« Incident relatif aux données personnelles »** a le sens attribué par les lois sur la protection des données aux termes « Incident de sécurité », «Violation de sécurité » ou « Violation des données personnelles » et comprend toute situation dans laquelle Entrust a connaissance du fait que des données personnelles ont été ou sont susceptibles d'avoir été consultées, divulguées, modifiées, perdues, détruites ou utilisées par des personnes non autorisées, de manière non autorisée.

**« Traitement »** signifie toute opération ou ensemble d'opérations effectuées sur des données personnelles, que ce soit ou non 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 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 que ces lois sont respectées. La Société y parvient en :

- mettant en œuvre des politiques qui permettent à la Société de se conformer aux lois sur la protection des données, telles que la présente politique, les politiques autour de la conservation des documents et de la sécurité des données, et les déclarations de confidentialité d'Entrust
- en communiquant avec les employés, les employés externes et les tiers agissant au nom d'Entrust et en les formant aux exigences en matière de protection des données
- En enquêtant sur les cas de non-conformité avec la politique de protection des données d'Entrust et en prenant les mesures correctives et/ou disciplinaires appropriées
- En enquêtant, en remédiant et, dans certains cas, en fournissant la notification d'un incident lié aux données personnelles

- en réalisant, le cas échéant, des évaluations sur les conséquences du traitement des données pour de nouveaux types d'activités de traitement
- En entreprenant des audits internes périodiques des politiques et procédures de protection des données d'Entrust
- en tenant compte de la protection des données dès le début de la conception des nouveaux produits

## 3.3 Traitement des données personnelles

Toutes les données personnelles traitées par la Société ou pour le compte d'Entrust doivent :

- être traitées de manière équitable, légale et transparente
- être traitées uniquement pour des raisons spécifiques, explicites et légitimes
- être pertinentes et se limiter aux seules nécessités de la ou des finalités légitimes pour lesquelles elles sont traitées
- être exactes et tenues 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 les objectifs pour lesquels elles ont été collectées
- être traitées de manière à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illégal, la perte accidentelle, la destruction ou les dommages

## 3.4 Traitement des données sensibles et de catégorie spéciale

Entrust traite des informations sensibles pour le compte de ses collaborateurs à travers divers systèmes d'entreprise et des données de catégorie spéciale limitées dans Workday. Des contrôles appropriés sont en vigueur et décrits dans les DPIA sur les données de catégorie spéciale, les avantages sociaux et la rémunération, ainsi que dans la norme de contrôle d'accès aux données sensibles et de catégorie spéciale disponible sur le site SharePoint d'Entrust Compliance.

## 3.5 Motifs juridiques du traitement des données personnelles

La Société ne peut traiter les données personnelles que si elle est autorisée à le faire en vertu des lois sur la protection des données.

Entrust traite les données personnelles :

- pour l'exécution d'un contrat auquel la personne concernée fait partie, ou pour prendre des mesures à la demande de la personne concernée avant la signature d'un contrat
- pour se conformer à une obligation légale à laquelle Entrust est soumise, y compris, mais sans s'y limiter, les demandes légales des autorités chargées de l'application de la loi
- pour servir les intérêts légitimes d'Entrust, sauf si ces intérêts sont supplantés par les intérêts ou les droits et libertés fondamentaux de la personne concernée

Outre ces motifs, Entrust peut également traiter des données à caractère personnel lorsque la personne concernée a donné son consentement au traitement pour une ou plusieurs raisons spécifiées, à condition que le consentement soit librement donné, spécifique, éclairé et qu'il constitue une indication non ambiguë des souhaits de la personne concernée. Lorsque Entrust utilise le consentement comme motif de traitement, une personne concernée a le droit de retirer son consentement à tout moment et pour toute raison.

Entrust peut, à l'occasion, également avoir besoin de traiter des catégories particulières de données personnelles pour les clients, les employés ou les travailleurs occasionnels (par exemple, si les pratiques de sécurité de l'emploi 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 particulière de données à caractère personnel pour une ou plusieurs raisons déterminées
- le traitement est nécessaire à l'exécution des obligations découlant du droit du travail, du droit de la sécurité sociale ou de la protection sociale ou d'une convention collective
- le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, ou de l'évaluation de la capacité de travail d'un employé
- le traitement est nécessaire à la sauvegarde des 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 porte sur des données à caractère personnel qui ont été rendues publiques par la personne concernée
- le traitement est nécessaire pour la constatation ou la défense de droits en justice

## 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 motifs lors de la première collecte des données ou, en cas d'impossibilité, dans les meilleurs délais par la suite.

Entrust ne traitera les données personnelles que dans la mesure requise et pour les besoins fournis à la personne concernée. Ceci signifie qu'Entrust ne peut 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 la Politique globale de gestion des documents et le Calendrier de conservation des documents qui l'accompagne.

## 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 des informations

Lorsque la société traite des données personnelles, elle prend des mesures raisonnables pour s'assurer que celles-ci demeurent sécurisées et protégées contre tout traitement non autorisé ou illégal, toute perte accidentelle, toute destruction ou tout dommage. Entrust applique ces mesures en :

- chiffrant les données personnelles lorsque cela est possible et approprié
- en garantissant la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services utilisés pour traiter les données personnelles
- en garantissant le rétablissement de l'accès aux données personnelles en temps utile en cas d'incident physique ou technique
- en facilitant les tests, l'évaluation et l'appréciation de l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité des données

Pour évaluer le niveau de sécurité approprié, 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 engage des tiers pour traiter des données personnelles en son nom, ces derniers agissent sur demande écrite, sont soumis à un devoir de confidentialité et sont tenus de mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité

des données conformément aux exigences de sécurité d'Entrust. Les données personnelles ne peuvent être partagées avec quiconque en dehors d'Entrust ou avec des tiers non autorisés.

Les bureaux et les 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 lié aux données personnelles peut se produire de plusieurs façons, notamment :

- la perte d'un périphérique mobile ou d'un fichier papier contenant des données personnelles (par exemple, l'abandon accidentel d'un périphérique dans les transports publics)
- le vol d'un périphérique mobile ou d'un fichier papier contenant des données à caractère personnel (par exemple, vol dans un véhicule ou à domicile)
- une erreur humaine (par exemple, l'envoi accidentel par un employé d'un courrier électronique contenant des données personnelles à un destinataire inapproprié, ou la modification ou la suppression accidentelle de données personnelles)
- une cyberattaque (par exemple, l'ouverture d'une pièce jointe à un courriel provenant d'un tiers inconnu et contenant un programme rançonneur ou un autre programme malveillant)
- l'autorisation d'une utilisation ou d'un accès non autorisé (par exemple, permettre à un tiers non autorisé d'accéder à des zones sécurisées des bureaux ou des systèmes d'Entrust)
- des circonstances imprévues telles qu'un incendie ou une inondation
- lorsqu'un tiers obtient des informations d'Entrust par la ruse

Un incident relatif aux données personnelles est susceptible de s'être produit dans les cas suivants :

- une ouverture de session inhabituelle et/ou une activité excessive du système, en particulier en ce qui concerne les comptes d'utilisateurs actifs
- une activité d'accès à distance inhabituelle
- la présence de réseaux sans fil (Wi-Fi) usurpés, visibles ou accessibles depuis l'environnement de travail d'Entrust
- la défaillance de l'équipement
- des logiciels ou matériels enregistreurs de saisie de texte connectés aux systèmes d'Entrust ou installés sur ceux-ci

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 Centre des opérations de sécurité (Entrust Security Operation Center) par courrier électronique à l'adresse SOC@entrust.com et l'équipe chargée de la conformité à l'adresse privacy@entrust.com.

## 3.10 Plan de réponse aux incidents concernant les 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 consistera à :

- enquêter sur l'incident pour déterminer la nature, la cause et l'étendue des dommages ou des préjudices qui peuvent en résulter
- mettre en œuvre les mesures nécessaires pour empêcher que l'incident ne se poursuive ou ne se reproduise, et limiter le préjudice subi par les 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) et effectuer ces notifications. S'il existe une obligation de notifier les autorités de protection des données, la notification doit généralement avoir lieu dans les 72 heures suivant la prise de connaissance de l'incident par la société, y compris par l'un de ses employés
- Enregistrement des informations concernant l'incident relatif aux données personnelles et les mesures prises en réponse, y compris la documentation expliquant la décision de notifier ou de ne pas notifier.

## 3.11 Stockage et sauvegarde des données personnelles

Entrust utilise plusieurs sites de serveurs pour stocker et sauvegarder les données personnelles. Pour les emplacements de serveurs utilisés par des tiers avec lesquels Entrust s'engage à traiter des données personnelles au nom de collègues et de clients, consultez les évaluations d'impact sur la protection des données pertinentes pour les données personnelles des collaborateurs et la page du sous-traitant externe et les avis de confidentialité des produits pour les données personnelles des clients. Ces documents sont tous situés soit en interne sur la page Conformité, soit en externe sur le site Droits et conformité sous les icônes 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 ») lorsqu'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 entreprises du groupe Entrust (c'est-à-dire toutes les personnes morales et les filiales) doivent conclure l'Accord de transfert de données intra-groupe afin de garantir des garanties

appropriées pour le transfert de données personnelles en dehors de l'EEE, mais au sein du groupe Entrust.

Les sociétés extérieures au groupe Entrust qui traitent des données personnelles pour ou au nom d'Entrust, pour lesquelles Entrust agit en tant que contrôleur de données ou gestionnaire de données, doivent conclure un accord de traitement de données avec Entrust afin de garantir des garanties appropriées pour le transfert de données personnelles en dehors de l'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.

Entrust peut transférer des données personnelles vers un pays situé en dehors de l'EEE dans les cas suivants :

- la personne concernée a donné son consentement explicite au transfert proposé après qu'Entrust l'ait informée des risques éventuels liés à ce transfert (par exemple, l'absence dans ce pays de garanties équivalentes)
- le transfert est nécessaire à la réalisation d'un contrat auquel la personne concernée fait partie ou pour prendre des mesures à la demande de la personne concernée avant de conclure un contrat
- le transfert est nécessaire à la sauvegarde des 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 transfert est nécessaire pour la constatation ou la défense d'un droit 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/EC, 2004/915/ECE et 2010/87/EU). Veuillez noter qu'un accord de transfert de données est également requis en cas de transfert de 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 nécessité et la base juridique du traitement des données personnelles
- l'éventuelle divulgation des données personnelles à des tiers au cours du traitement
- l'éventualité d'un transfert de données personnelles en dehors de l'EEE et du Canada et, dans l'affirmative, les mesures de protection qui seront mises en place

- la durée de traitement des données personnelles ou, s'il n'est pas possible de la déterminer, les critères utilisés par la société pour déterminer la période de traitement
- la manière dont la personne concernée peut obtenir une copie de ses données personnelles détenues par Entrust
- les droits de la personne concernée, y compris la manière de déposer une plainte
- l'éventualité que les données personnelles doivent être traitées pour se conformer à une loi ou à un contrat, les conséquences possibles du fait que la personne concernée ne fournisse pas les données ou s'oppose au traitement
- l'existence et les modalités de tout processus décisionnel automatisé, le cas échéant

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

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

## 3.14 Privacy by Design (autrement dit protection de la vie privée intégrée dans les nouvelles applications technologiques et commerciales dès leur conception) et évaluations de l'impact sur 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 objectifs pour lesquels l'activité est menée, la manière dont Entrust se conformera aux lois sur la protection des données et la manière dont la société atténuera les risques potentiels pour la vie privée des personnes. Si vous pensez qu'une évaluation de l'impact sur la protection des données est nécessaire, contactez le Vice-Président chargé de la conformité à l'adresse privacy@entrust.com.

## 3.15 Droits de la personne concernée

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

- demander des informations sur les données personnelles détenues à son sujet

- faire rectifier les données personnelles inexactes la concernant et faire compléter les données personnelles incomplètes, sous réserve qu'Entrust détermine que les données sont, en fait, inexactes ou 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 malgré une objection si les intérêts légitimes de la Société l'emportent sur ceux de la personne concernée, ou si Entrust y a recours pour l'établissement ou le recouvrement d'une réclamation légale
- 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 pour les raisons pour lesquelles elles sont traitées et s'il existe une base légitime pour Entrust de poursuivre le processus
- La personne concernée peut demander à Entrust de limiter le traitement de ses données personnelles à leur stockage. Cette demande ne peut être formulée 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 réclamation légale ; la personne concernée s'est opposée au traitement de ses données personnelles ; et Entrust décide si ses intérêts légitimes prévalent sur les intérêts de la personne concernée ou si le traitement est illégal

Entrust évaluera au cas par cas les droits de la personne concernée en vertu de la législation applicable en matière de confidentialité des données pour 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 fournit à tous les employés et collaborateurs externes une formation obligatoire sur les responsabilités en matière de protection des données. Cette présentation de la formation sur la

confidentialité des données a lieu au moment de l'intégration et à intervalles réguliers par la suite. En plus de la présentation de la formation sur la confidentialité des données pour tous les collègues, Entrust fournit une formation renforcée sur la confidentialité des données aux employés qui traitent des données de catégorie spéciale et une formation sur le concept Privacy by Design aux employés qui développent de nouveaux produits et offres de services. Nous continuons à développer et à déployer d'autres formations sur la confidentialité spécifiques aux fonctions, en fonction des besoins.

## 3.18 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 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, VP de la conformité
1187 Park Place
Shakopee, MN 55379
privacy@entrust.com

Le préposé à la protection des données désigné par Entrust Deutschland GmbH est M. Niels Kill de 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 Directeur des affaires juridiques et de la conformité. 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 de la personne à contacter

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.