POLITIQUE GLOBALE DE PROTECTION DES DONNEES PERSONNELLES

Version du document	1.2
Date	10 septembre 2020

TABLE DES MATIÈRES

1 INTRODUCTION

En tant qu'entreprise et employeur, Entrust Corporation et ses filiales et sociétés affiliées (collectivement, « Entrust » ou la « Société ») doivent recueillir, stocker et traiter des données personnelles sur nos employés, nos intérimaires, nos clients, nos fournisseurs et les autres tiers avec lesquels nous faisons affaire pour fournir des produits ou services pour notre compte.

Avec l'introduction du Règlement général 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 accrues concernant la manière dont nous collectons, utilisons et conservons 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 à propos desquelles nous détenons des données personnelles d'avoir confiance en nous. La présente politique s'applique à tous les employés d'Entrust, aux intérimaires et aux tiers qui traitent des données au nom d'Entrust. Sauf indication contraire, la présente politique s'applique dans tous les pays où Entrust exerce ses activités.

3 EXIGENCES DE LA POLITIQUE

3.1 DÉFINITIONS

« Contrôleur de données » désigne l'entité qui détermine la nécessité et les moyens de traitement des données personnelles.

« Responsable du traitement des données » désigne l'entité qui traite les données à caractère personnel au nom du contrôleur.

« Lois sur la protection des données » désigne l'ensemble des lois et règlementations 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, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) du Canada et la Consumer Privacy Act (CCPA) de Californie.

« Personne concernée » désigne la personne identifiée ou identifiable ou le ménage auquel se rapportent les données à caractère personnel.

« Utilisateur de données » est un terme utilisé pour décrire tout employé, consultant, entrepreneur indépendant, stagiaire, travailleur temporaire ou tiers agissant pour le compte d'Entrust (y compris les sous-traitants) dont le travail implique le traitement de données à caractère personnel pour Entrust.

« Données personnelles » a la même signification attribuée aux « informations personnellement identifiables », « informations personnelles »,« données personnelles » ou des termes équivalents tels que ceux définis par les lois sur la protection des données.

« Incident de données personnelles » a la même signification que les termes que les lois sur la protection des données attribuent aux termes « incident de sécurité »,« violation de la sécurité » ou « violation des données personnelles » et doit inclure toute situation dans laquelle le vendeur prend connaissance que des données personnelles ont été ou sont susceptibles d'avoir été consultées, divulguées, altérées, perdues, détruites ou utilisées par des personnes non autorisées, de manière non autorisée.

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

« Les données de catégorie spéciale » sont un sous-ensemble de données personnelles et se réfèrent 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), ses antécédents médicaux, son casier judiciaire et toutes les mesures de sécurité connexes dont il pourrait faire l'objet.

3.2 NOTRE RESPONSABILITÉ

Selon les circonstances, Entrust peut agir à titre de contrôleur ou de processeur de données. En tant que responsable du traitement des données, l'entreprise Entrust est chargée 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 sa conformité à ces lois. Pour ce faire, la Société s'engage à :

- Mettre en œuvre des politiques qui permettent à la Société de se conformer aux lois sur la protection des données comme la présente politique, aux politiques sur la conservation et la sécurité des documents et des données et aux déclarations de confidentialité d'Entrust ;
- Communiquer et former les employés, les intérimaires et les tiers agissant au nom d'Entrust au sujet des exigences en matière de protection des données ;
- Enquêter sur les cas de non-conformité aux politiques de protection des données d'Entrust et prendre les mesures correctives ou disciplinaires appropriées ;
- enquêter, remédier et, dans certains cas, notifier un incident concernant des données à caractère personnel ;

- réaliser des analyses d'impact du traitement des données lorsque cela est nécessaire pour de nouveaux types de traitement ;
- entreprendre des audits internes périodiques des politiques et procédures de protection des données d'Entrust ; et
- Prise en 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 l'entreprise traite ou qui sont traitées pour le compte d'Entrust doivent :

- être traitées équitablement, légalement et de manière transparente ;
- être traitées uniquement à des fins précises, explicites et légales.
- être pertinentes et limitées à ce qui est nécessaire pour la ou les finalités légitimes pour lesquelles les données sont traitées ;
- être exactes et tenues à jour, en veillant, dans la mesure du possible, à ce que les données à caractère personnel inexactes soient effacées ou rectifiées sans délai ;
- ne pas être conservées plus longtemps que nécessaire pour remplir la ou les finalités pour lesquelles les données ont été collectées ; et
- être traitées de manière à assurer une sécurité appropriée des données à caractère personnel, y compris la protection contre tout traitement non autorisé ou illicite, toute perte accidentelle, toute destruction ou tout dommage.

3.4 MOTIFS JURIDIQUES DU TRAITEMENT DES DONNEES 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. Voici les motifs sur lesquels Entrust s'appuie pour traiter les données personnelles :

Lorsque le traitement est nécessaire :

- à l'exécution d'un contrat auquel la personne concernée est une partie ou pour répondre à une demande de la personne concernée avant la passation d'un contrat ;
- au respect d'une obligation légale à laquelle Entrust est soumise ; et/ou
- poursuivre les intérêts légitimes d'Entrust, sauf lorsque les intérêts ou les droits et libertés fondamentaux de la personne concernée l'emportent sur ces intérêts.

Outre ces motifs, Entrust peut également traiter des données personnelles lorsque la personne concernée a donné son consentement pour une ou plusieurs finalités déterminées, à condition que ce consentement soit donné librement, de manière spécifique, éclairée et sans ambiguïté. Lorsqu'Entrust utilise le consentement comme motif de traitement, la personne concernée a le droit de retirer son consentement en tout temps et pour toute raison.

Entrust peut, à l'occasion, avoir à traiter des catégories particulières de données personnelles concernant des employés ou des intérimaires (par exemple lorsque des pratiques d'emploi sécuritaires l'exigent). Lorsqu'Entrust traite ou fait appel à 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 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 de travail ;
- le traitement est nécessaire à des fins de médecine préventive ou de médecine du travail, ou pour l'évaluation de la capacité de travail d'un salarié ;
- le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée ou d'une autre personne lorsque celle-ci est physiquement ou juridiquement incapable de donner son consentement ;
- le traitement concerne des données à caractère personnel qui ont été rendues publiques par la personne concernée ; et/ou
- le traitement est nécessaire à l'établissement ou à la défense d'actions en justice

3.5 GESTION DES ENREGISTREMENTS DE DONNÉES

Entrust conserve un registre central des types de données personnelles que l'entreprise collecte, ainsi que les raisons pour lesquelles ces données sont collectées. Entrust ne traitera les données à caractère personnel que dans le(s) but(s) spécifique(s) indiqué(s) dans le registre central ou pour tout autre but spécifiquement autorisé par les lois sur la protection des données. Entrust informera les personnes concernées de ces fins lorsque les données seront collectées pour la première fois ou, si cela n'est pas possible, dès que possible par la suite.

Entrust ne traitera les données personnelles que dans la mesure nécessaire aux fins pour lesquelles elles ont été 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 s'assurer que les données personnelles qui ne sont plus nécessaires sont effacées ou détruites.

La Société emploie également des mesures raisonnables pour s'assurer que toutes les données personnelles détenues sont exactes et à jour. Entrust vise à vérifier l'exactitude de toute donnée personnelle au point de collecte et à intervalles réguliers par la suite. La société prendra toutes les mesures raisonnables pour effacer, détruire ou modifier les données inexactes ou périmées sans délai excessif 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 lorsqu'il existe des raisons spécifiques pour lesquelles un mois n'est pas possible).

3.6 EFFACEMENT OU DESTRUCTION DES DONNEES A CARACTERE PERSONNEL

Les documents papier qui contiennent des données personnelles doivent être détruits et éliminés de façon sécuritaire lorsqu'il n'est plus nécessaire de les conserver. Les documents papier contenant des données à caractère personnel ne peuvent être éliminés d'aucune autre manière.

Lors de la suppression de données électroniques à caractère personnel, toutes les mesures possibles devraient être prises pour mettre les données en question hors d'usage. Lorsqu'il est impossible de supprimer complètement des données à caractère personnel, des mesures raisonnables doivent être prises pour garantir que les données soient 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 à caractère personnel (par exemple, ordinateurs portables, ordinateurs de bureau, périphériques mobiles appartenant à l'entreprise et données de travail sur les appareils BYOD).

3.7 SÉCURITÉ DES INFORMATIONS

Lorsque l'entreprise traite des données personnelles, elle prend des mesures raisonnables pour s'assurer que les données restent sécurisées et qu'elles sont protégées contre tout traitement non autorisé ou illégal, perte accidentelle, destruction ou dommage. Pour ce faire, Entrust prend les mesures suivantes :

- le cryptage des données personnelles lorsque cela est possible et approprié ;
- garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des 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'appréciation et l'évaluation de l'efficacité des mesures techniques et organisationnelles visant à assurer la sécurité des données.

Pour évaluer le niveau de sécurité approprié, Entrust tient compte des risques associés au traitement, en particulier les risques de destruction accidentelle ou illicite, de perte, d'altération, de divulgation non autorisée ou d'accès non autorisé aux données personnelles qui sont 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 tenues au secret professionnel et sont tenues de prendre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données. Les données personnelles ne peuvent être partagées avec aucune personne n'appartenant pas à Entrust ou de tierces parties autorisées.

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 écrans individuels ne montrent pas de données personnelles ou d'informations confidentielles aux passants et qu'ils se déconnectent ou verrouillent leurs ordinateurs ou tablettes lorsqu'ils sont laissés sans surveillance.

3.8 SIGNALER UN INCIDENT RELATIF AUX DONNEES 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 en laissant accidentellement un périphérique dans les transports publics) ;
- le vol d'un périphérique mobile ou d'un fichier papier contenant des données personnelles (par exemple en cas de vol dans un véhicule ou à domicile) ;
- une erreur humaine (par exemple si un employé envoie accidentellement un courrier électronique contenant des données personnelles à un destinataire imprévu ou modifie ou supprime accidentellement des données personnelles) ;
- Cyber-attaque (par exemple l'ouverture d'une pièce jointe à un courrier électronique provenant d'un tiers inconnu qui contient un logiciel de rançon ou un autre logiciel malveillant) ;
- Permettre l'utilisation ou l'accès non autorisés (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 ; ou
- lorsqu'une tierce partie a obtenu des informations d'Entrust au moyen d'une supercherie.

Les signes indiquant qu'un incident lié aux données personnelles a pu se produire sont notamment les suivants :

- une connexion inhabituelle et/ou une activité excessive du système, en particulier en ce qui concerne les comptes utilisateurs actifs ;
- une activité inhabituelle d'accès à distance ;
- La présence de réseaux sans fil usurpés (Wi-Fi) visibles ou accessibles à partir de l'environnement de travail d'Entrust ;
- une panne d'équipement ; et
- Enregistreurs de clés matériels ou logiciels connectés ou installés sur les systèmes Entrust.

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

3.9 PLAN D'INTERVENTION EN CAS D'INCIDENT CONCERNANT LES DONNEES A CARACTERE PERSONNEL

En cas d'incident réel ou imminent concernant des données personnelles, Entrust prend rapidement des mesures pour minimiser l'impact de l'incident et le signaler 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 qui peuvent en résulter ;
- appliquer les mesures nécessaires pour empêcher que l'incident ne se poursuive ou ne se reproduise, et limiter les dommages aux personnes concernées ;
- d'évaluer s'il existe une obligation de notification à d'autres parties (par exemple, les autorités nationales chargées de la protection des données, les personnes concernées) et effectuer ces notifications. S'il existe une obligation de notification aux autorités de protection des données, la notification doit généralement avoir lieu dans les 72 heures suivant la prise de connaissance de l'incident par l'entreprise, y compris par l'un de ses employés ; et
- les informations d'enregistrement sur l'incident relatif aux données à caractère personnel et les mesures prises en conséquence, y compris la documentation qui explique la décision de notifier ou de ne pas notifier.

3.10 TRANSFERTS INTERNATIONAUX DE DONNEES ET TRANSFERTS A DES TIERS

Dans le cadre du RGPD, Entrust peut transférer des données personnelles vers des pays situés à l'extérieur 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 sociétés du groupe Entrust (c'est-à-dire toutes les sociétés et filiales) doivent conclure l'accord de transfert de données intragroupe afin de garantir des garanties appropriées pour le transfert de données à caractère personnel 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 à titre de responsable du traitement des données ou de sous-traitant, doivent conclure un accord de traitement des données avec Entrust afin d'assurer des garanties appropriées pour le transfert des données personnelles en dehors de l'EEE. Cet accord contient des dispositions visant à garantir que le tiers dispose des mesures techniques et organisationnelles appropriées pour se conformer au RGPD et assurer 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 :

- que la personne concernée a donné son consentement explicite au transfert proposé après qu'Entrust l'ait informée des risques éventuels associés à ce transfert (par exemple l'absence de garanties équivalentes dans ce pays) ;
- le transfert est nécessaire à l'exécution d'un contrat auquel la personne concernée est une partie ou à la prise de mesures à la demande de la personne concernée avant la conclusion du contrat ;
- le transfert est nécessaire à la protection des intérêts vitaux de la personne concernée ou d'une autre personne lorsque celle-ci est physiquement ou juridiquement incapable de donner son consentement ; ou

- le transfert est nécessaire pour l'établissement ou la défense d'une réclamation légale.

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/EC et 2010/87/EU). Veuillez noter qu'un accord de transfert de données est également requis si vous transférez des données personnelles en-dehors du Canada.

3.11 NOTIFICATION AUX PERSONNES CONCERNÉES

Entrust est tenue de fournir aux personnes concernées des informations sur le traitement de leurs données personnelles. Ces informations sont contenues dans la déclaration de confidentialité de la Société, qui est accessible au public à l'adresse www.entrust.com, et dans la déclaration de confidentialité des employés, qui est disponible sur l'intranet d'Entrust. Ces déclarations fournissent des informations sur les noms de domaine concernant :

- les types de données personnelles traitées par Entrust ;
- la finalité et base juridique du traitement des données à caractère personnel ;
- si des données personnelles seront divulguées à des tiers au cours du traitement ;
- si les données personnelles seront transférées à l'extérieur de l'EEE et du Canada et, le cas échéant, quelles mesures de protection seront mises en place ;
- la durée du traitement des données personnelles ou, s'il n'est pas possible de le déterminer, les critères que la Société utilisera pour déterminer la période de traitement ;
- comment 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 réclamation ;
- si les données à caractère personnel doivent être traitées afin de respecter une loi ou un contrat, les conséquences éventuelles du fait que la personne concernée ne fournit pas les données ou s'oppose au traitement ; et
- l'existence et les détails de tout processus décisionnel automatisé, le cas échéant.

Si Entrust reçoit des données personnelles concernant un individu de la part d'un tiers, l'entreprise fournira également à cette dernière des renseignements sur :

- le type de données personnelles reçues de la tierce partie ; et
- la source des données et si elles proviennent d'une source accessible au public (par exemple un site Web accessible au public).

3.12 ÉVALUATIONS D'IMPACT SUR LA PROTECTION DE LA VIE PRIVEE ET DES DONNEES

Les lois sur la protection des données exigent qu'Entrust prenne en considération la protection des données pendant les étapes de développement d'une nouvelle offre de produits. Pour s'acquitter de 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 réduite au minimum dans la mesure du possible.

Dans certaines circonstances (notamment lorsque le traitement entraînerait un risque élevé pour les droits et libertés d'une personne), Entrust peut être tenue de procéder à une évaluation officielle des répercussions sur la protection des données (EIPD) relativement au traitement des données personnelles. Une telle évaluation consiste à documenter les fins pour lesquelles l'activité est menée, la façon dont Entrust se conformera aux lois sur la protection des données et la façon dont la Société atténuera les risques potentiels pour la vie privée des personnes. Si vous pensez qu'une étude d'impact sur la protection des données est nécessaire, veuillez contacter le Directeur du service de la conformité à l'adresse privacy@entrust.com.

3.13 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 les concernant ;
- faire corriger les données personnelles inexactes ou incomplètes à leur sujet, sous réserve qu'Entrust détermine que les données sont effectivement inexactes ou incomplètes ;
- s'opposer à ce qu'Entrust traite leurs données personnelles lorsque la Société le fait dans le respect de ses propres intérêts légitimes. Entrust peut continuer à traiter les données personnelles en dépit d'une objection si les intérêts légitimes de la Société l'emportent sur ceux de la personne concernée, ou si Entrust doit le faire pour établir ou défendre une réclamation 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 s'il existe une base légitime pour qu'Entrust puisse poursuivre le traitement ;
- Demander à Entrust de limiter le traitement de leurs données personnelles au stockage. Cela ne peut être demandé que si l'exactitude des données personnelles a été contestée et n'est pas 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 ou si ce traitement est illicite.

Si une personne concernée exerce ces droits et qu'Entrust a communiqué les données personnelles en question à un tiers, la Société fera de son mieux pour s'assurer que ce tiers respecte également les souhaits de la personne concernée.

3.14 DEMANDES D'ACCÈS DES PERSONNES CONCERNÉES

Les personnes concernées qui souhaitent obtenir des renseignements sur les données personnelles qu'Entrust détient à leur sujet peuvent le faire en soumettant une demande d'accès à leurs données personnelles (DSAR) disponible à l'adresse https://www.entrust.com/data-privacy-management. Si les collègues reçoivent une demande directement (que ce soit verbalement ou par écrit), ils doivent immédiatement transmettre les détails de la demande à privacy@entrust.com.

3.15 FORMATION

Entrust offre à ses employés et à ses intérimaires une formation sur les responsabilités en matière de protection des données. Cette formation a lieu au moment de l'embauche et à intervalles réguliers par la suite.

3.16 RESPONSABLE DE LA PROTECTION DES DONNEES

Le représentant d'Entrust affecté au département RGPD est Anjali Doherty, Sr. Directeur des affaires juridiques de l'entreprise (Royaume-Uni). Le responsable de la protection des données d'Entrust Deutschland GmbH est le cabinet d'avocats de Kill & Wolff GmbH. Entrust Corporation n'a pas de délégué affecté à la protection des données. La surveillance du programme de conformité en matière de protection des données est assurée par la directrice de la Conformité, Jenny Carmichael, qui se trouve au siège social d'Entrust à Shakopee, au Minnesota, aux États-Unis.

4 CONFORMITÉ

Tous les employés et intérimaires sont tenus de se conformer à cette politique. De plus, toutes les unités d'affaires doivent s'assurer qu'elles ont mis en place des normes et des procédures locales appropriées pour se conformer à cette politique et à la législation applicable en matière de protection des données dans leur juridiction. Tout manquement à cette politique sera pris au sérieux et peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. Cette politique peut être mise à jour ou modifiée à tout moment.

5 EXCEPTIONS

Il n'existe aucune exception à cette politique.

6 PROPRIÉTÉ ET RÉVISION

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

6.1 COORDONNÉES

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