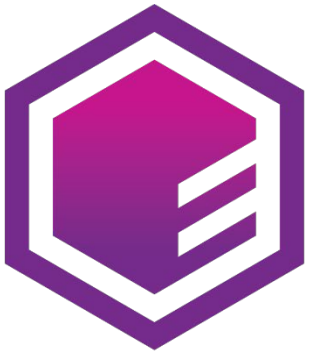

ENTRUST

POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS

Versão do documento	1.4
Data	10-dez-2021

Índice

1. Introdução

Como uma empresa e um empregador, é necessário que a Entrust Corporation e suas subsidiárias e afiliadas (coletivamente, "Confiar" ou a "Empresa") coletem, armazenem e processem dados pessoais sobre nossos funcionários, trabalhadores contingentes, clientes, fornecedores e outros terceiros com os quais nos comprometemos a fornecer produtos ou serviços em nosso nome.

Com a introdução do Regulamento Geral Europeu de Proteção de Dados ("GDPR") em 25 de maio de 2018 e outras leis aplicáveis que regem a proteção de dados, estamos sujeitos a requisitos aprimorados quanto à forma como coletamos, usamos e armazenamos dados pessoais.

2. Objetivo

O objetivo desta política é ajudar a todos nós a cumprir nossas obrigações legais e permitir que os indivíduos sobre os quais temos dados pessoais tenham confiança em nós. Esta política se aplica a todos os funcionários da Confiança, trabalhadores contingentes e terceiros que processam dados em nome da Confiança. A menos que especificado, esta política se aplica em todos os países nos quais a Trust opera e/ou conduz negócios.

3. Exigências políticas

3.1 Definições

"Controlador de dados" ou **"Controlador de informações pessoais identificáveis (Controlador PII)"** significa a entidade que determina a finalidade e os meios de processamento de dados pessoais.

"Processador de dados" ou **"Processador de informações pessoais identificáveis (Processador PII)"** significa a entidade que processa os dados pessoais em nome do Controlador.

"Data Protection Laws" significa todas as leis e regulamentos aplicáveis de proteção e privacidade de dados, incluindo mas não se limitando à Regulamentação Geral de Proteção de Dados da UE (GDPR), Regulamentação Geral de Proteção de Dados do Reino Unido (UK GDPR), Lei de Proteção de Informações Pessoais e Documentos Eletrônicos do Canadá (PIPEDA), e a Lei de Privacidade do Consumidor da Califórnia (CCPA)

"Sujeito dos Dados" ou **"Personally Identifiable Information Principal (PII Principal)"** significa a pessoa ou domicílio identificado ou identificável a quem os Dados Pessoais se referem.

"Data User" é um termo usado para descrever qualquer funcionário, consultor, contratado independente, estagiário, trabalhador temporário ou terceiro agindo em nome do Trust

(incluindo processadores de dados) cujo trabalho envolva o processamento de dados pessoais para o Trust

"Dados pessoais" terá o significado atribuído a "informações pessoalmente identificáveis", "informações pessoais", "dados pessoais" ou termos equivalentes, conforme tais termos são definidos sob as Leis de Proteção de Dados

"Incidente de Dados Pessoais" terá o significado atribuído pelas Leis de Proteção de Dados aos termos "incidente de segurança", "violação de segurança" ou "violação de dados pessoais" e incluirá qualquer situação na qual o Entrust tome conhecimento de que os Dados Pessoais foram ou podem ter sido acessados, divulgados, alterados, perdidos, destruídos ou usados por pessoas não autorizadas, de forma não autorizada

"Processamento" significa qualquer operação ou conjunto de operações que seja realizada sobre Dados Pessoais, seja ou não por meios automáticos, tais como coleta, registro, estruturação organizacional, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição O processamento também inclui a transferência ou divulgação de dados pessoais a terceiros.

"Special Category Data" ou **"Special Category Personal Information"** é um subconjunto de dados pessoais e refere-se a informações sobre a raça ou origem étnica, vida sexual ou orientação sexual de um indivíduo, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos (cor dos olhos, cor do cabelo, altura, peso), histórico médico, ou condenações e delitos criminais ou medidas de segurança relacionadas.

3.2 Nossa responsabilidade

Dependendo das circunstâncias, a Confiança pode agir como um controlador de dados ou um processador de dados. Como responsável pelo controle de dados, a Confiança é responsável por estabelecer práticas e políticas em conformidade com as Leis de Proteção de Dados. É igualmente importante que a empresa Trust seja capaz de demonstrar o cumprimento dessas leis. A Empresa faz isto por:

- Implementar políticas que permitam à empresa cumprir as leis de proteção de dados, tais como esta política, políticas sobre retenção de documentos e segurança de dados, e as declarações de privacidade da Confiust;
- Comunicação e treinamento de funcionários, trabalhadores contingentes e terceiros agindo em nome da Confiança sobre os requisitos de proteção de dados;
- Investigar casos de não conformidade com as políticas de proteção de dados de Confiança e tomar as medidas corretivas e/ou disciplinares apropriadas;
- Investigando, remediando e, em alguns casos, fornecendo notificação de um Incidente de Dados Pessoais;
- Realização de avaliações de impacto do processamento de dados quando necessário para novos tipos de atividades de processamento;

- Realizar auditorias internas periódicas das políticas e procedimentos de proteção de dados da Confiust; e
- Considerando a proteção de dados no início da concepção de novos produtos.

3.3 Processamento de dados pessoais

Quaisquer dados pessoais que a empresa processe ou que sejam processados em nome da Confiança devem ser processados:

- Ser processado de forma justa, legal e transparente;
- Ser processado somente para fins específicos, explícitos e legítimos;
- Ser relevante e limitado ao necessário para a(s) finalidade(s) legítima(s) para a(s) qual(is) os dados são processados;
- Ser preciso e atualizado garantindo, quando razoavelmente possível, que dados pessoais imprecisos sejam apagados ou retificados sem demora;
- Não ser guardado por mais tempo do que o necessário para cumprir a(s) finalidade(s) para a qual os dados foram coletados; e
- Ser processados de forma a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal, perda acidental, destruição ou dano.

3.4 Processamento de dados sensíveis e de categoria especial

Confiar aos colegas informações sensíveis em nome dos colegas em vários sistemas empresariais e dados limitados de categoria especial no dia de trabalho. Os controles apropriados estão em vigor e descritos nos DPIAs de Categorias Especiais, Benefícios e Folha de Pagamento e no Padrão de Controle de Acesso para Dados Sensíveis e de Categorias Especiais disponíveis no site de Conformidade de Confiança.

3.5 Fundamentos legais para o processamento de dados pessoais

A Empresa só pode processar dados pessoais se for permitido fazê-lo de acordo com as Leis de Proteção de Dados. Os motivos a seguir são os fundamentos em que a Confiança se baseia para processar dados pessoais:

Onde o processamento é necessário:

- Para a execução de um contrato no qual o envolvido é parte ou para tomar medidas a pedido do envolvido antes de firmar um contrato;
- Para o cumprimento de uma obrigação legal à qual a Entrust está sujeita, incluindo, entre outros, solicitações legais de autoridades de aplicação da lei; e/ou
- Alcançar interesses legítimos do Trust, exceto quando tais interesses são anulados pelos interesses ou direitos e pelas liberdades fundamentais do envolvido.

Além destes fundamentos, o Trust também pode processar dados pessoais quando o envolvido tiver dado consentimento ao processamento para uma ou mais finalidades especificadas, desde

que o consentimento seja dado livremente, específico, informado e uma indicação inequívoca da vontade do envolvido. Nos casos em que o Entrust usa o consentimento como base para o processamento, o envolvido tem o direito de retirar o consentimento a qualquer momento e por qualquer motivo.

Ocasionalmente, a empresa pode também precisar processar categorias especiais de dados pessoais para clientes, funcionários ou trabalhadores contingentes (por exemplo, quando exigido pelas práticas de emprego seguro). Quando o Grupo Trust processa ou utiliza terceiros para processar em seu nome categorias especiais de dados pessoais, o Grupo Trust assegurará, quando aplicável, que as seguintes condições sejam satisfeitas:

- O envolvido deu consentimento explícito para o processamento da categoria especial de dados pessoais para uma ou mais finalidades especificadas;
- O processamento é necessário para o cumprimento das obrigações previstas na legislação trabalhista, previdenciária ou de proteção social, ou em um acordo de negociação coletiva;
- O processamento é necessário para fins de medicina preventiva ou ocupacional, ou para a avaliação da capacidade de trabalho de um funcionário;
- O processamento é necessário para proteger os interesses vitais do envolvido ou de outra pessoa quando o envolvido for física ou legalmente incapaz de dar seu consentimento;
- O processamento refere-se a dados pessoais que tenham sido tornados públicos pelo envolvido; e/ou
- O processamento é necessário para o estabelecimento ou defesa de reivindicações legais.

3.6 Gerenciamento de registros de dados

A empresa mantém um registro central dos tipos de dados pessoais que a empresa coleta e porque esses dados são coletados. O responsável só processará dados pessoais para a(s) finalidade(s) específica(s) estabelecida(s) no registro central ou para qualquer outra(s) finalidade(s) especificamente permitida(s) pelas Leis de Proteção de Dados. A empresa encarregada notificará as pessoas em questão sobre essas finalidades quando os dados forem coletados pela primeira vez ou, quando não for possível, o mais rápido possível depois disso.

O responsável só processará os dados pessoais na medida do necessário para os fins fornecidos ao envolvido. Isto significa que a Confiança não pode pedir ou registrar em seus sistemas mais dados pessoais do que os necessários. A empresa tem medidas técnicas e organizacionais apropriadas para assegurar que os dados pessoais que não são mais necessários sejam apagados ou destruídos.

A empresa também emprega medidas razoáveis para assegurar que quaisquer dados pessoais mantidos sejam precisos e mantidos atualizados. O objetivo do Trust é verificar a exatidão de quaisquer dados pessoais no ponto de coleta e, em seguida, em intervalos regulares. A

Empresa tomará todas as medidas razoáveis para apagar, destruir ou alterar dados inexatos ou desatualizados sem demora indevida e, em qualquer caso, no prazo de um mês após a solicitação do interessado (ou até três meses quando houver razões específicas para que o período de um mês não seja possível).

Para mais informações sobre gerenciamento e retenção de registros, consulte a Política global de gestão de registros e o anexo Calendário de retenção de registros.

3.7 Apagamento ou destruição de dados pessoais

Os registros em papel que contêm dados pessoais devem ser triturados e descartados de forma segura quando não houver mais necessidade de retê-los. *Os registros em papel contendo dados pessoais não podem ser descartados de nenhuma outra forma.*

Ao apagar os dados pessoais eletrônicos, devem ser tomadas todas as medidas possíveis para colocar os dados em questão além do uso. Quando for impossível apagar dados pessoais por completo, devem ser tomadas medidas razoáveis para garantir que os dados sejam apagados na medida do possível.

A TI é responsável por destruir ou apagar equipamentos eletrônicos que contenham dados pessoais (por exemplo, laptops, desktops, dispositivos móveis da empresa e dados de trabalho em dispositivos BYOD).

3.8 Segurança da Informação

Quando a empresa processa dados pessoais, ela toma medidas razoáveis para garantir que os dados permaneçam seguros e protegidos contra processamento não autorizado ou ilegal, perda acidental, destruição ou dano. Confiar isto por:

- Criptografar dados pessoais sempre que possível e apropriado;
- Assegurar a contínua confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços usados para processar dados pessoais;
- Garantir a restauração do acesso aos dados pessoais em tempo hábil no caso de um incidente físico ou técnico; e
- Facilitando testes, avaliação e avaliação da eficácia das medidas técnicas e organizacionais para garantir a segurança dos dados.

Ao avaliar o nível apropriado de segurança, a Confissão considera os riscos associados ao processamento, em particular os riscos de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos dados pessoais que são processados.

Nos casos em que a empresa Encarregada contratar terceiros para processar dados pessoais em seu nome, tais partes o fazem com base em instruções escritas, estão sob um dever de confidencialidade e são obrigadas a implementar medidas técnicas e organizacionais apropriadas para garantir a segurança dos dados. Os dados pessoais não podem ser compartilhados com ninguém fora da Confiança ou de terceiros autorizados.

As escrivaninhas e armários são mantidos trancados se eles tiverem dados pessoais ou informações confidenciais de qualquer tipo. Os usuários de dados garantem que os monitores/telas individuais não mostrem dados pessoais ou informações confidenciais aos transeuntes e que eles façam log off ou bloqueiem seus computadores/tabelas quando deixados sem supervisão.

3.9 Relatar um incidente de dados pessoais

Um incidente de dados pessoais pode acontecer de muitas maneiras, inclusive:

- Perda de um dispositivo móvel ou arquivo de cópia impressa que contenha dados pessoais (por exemplo, deixar acidentalmente um dispositivo no transporte público);
- Roubo de um dispositivo móvel ou arquivo de cópia impressa que contenha dados pessoais (por exemplo, roubados de um veículo ou de uma casa);
- Erro humano (por exemplo, um funcionário enviando acidentalmente um e-mail contendo dados pessoais para um destinatário não intencional, ou alterando ou apagando acidentalmente dados pessoais);
- Ataque cibernético (por exemplo, abertura de um anexo a um e-mail de um terceiro desconhecido que contém um resgate ou outro malware);
- Permitir o uso/acesso não autorizado (por exemplo, permitir que um terceiro não autorizado tenha acesso a áreas seguras dos escritórios ou sistemas de Confiança);
- Circunstâncias imprevistas como um incêndio ou inundação; ou
- Onde a informação é obtida da Confiança por terceiros através de engano.

Os sinais de que um Incidente de Dados Pessoais pode ter ocorrido incluem o seguinte:

- Log-in incomum e/ou atividade excessiva do sistema, em particular no que diz respeito às contas de usuários ativos;
- Atividade inusitada de acesso remoto;
- A presença de redes sem fio falsificadas (Wi-Fi) visíveis ou acessíveis a partir do ambiente de trabalho da Confiust;
- Falha do equipamento; e
- Registradores de chaves de hardware ou software conectados ou instalados em sistemas de confiança.

Os colegas que tomem conhecimento ou tenham qualquer razão para suspeitar que um Incidente de Dados Pessoais tenha ocorrido ou esteja prestes a ocorrer devem contatar imediatamente o Centro de Operações de Segurança de Confiança pelo e-mail SOC@entrust.com e o Diretor de Conformidade pelo e-mail privacy@entrust.com.

3.10 Plano de Resposta a Incidentes com Dados Pessoais

No caso de um Incidente de Dados Pessoais real ou iminente, a Confiança toma uma ação rápida para minimizar o impacto do incidente e relatar o incidente se exigido por lei. Na maioria dos casos, a resposta envolverá:

- Investigar o incidente para determinar a natureza, causa e extensão dos danos ou prejuízos que possam resultar;
- Implementar as medidas necessárias para impedir que o incidente continue ou seja recorrente, e limitar os danos às pessoas afetadas;
- Avaliar se existe uma obrigação de notificar outras partes (por exemplo, autoridades nacionais de proteção de dados, pessoas afetadas) e fazer essas notificações. Se houver a obrigação de notificar as autoridades de proteção de dados, a comunicação deve normalmente ocorrer dentro de 72 horas após a empresa, incluindo qualquer um de seus funcionários, tomar conhecimento do incidente; e
- Registro de informações sobre o Incidente de Dados Pessoais e as medidas tomadas em resposta, incluindo documentação que explica a decisão de notificar ou não.

3.11 Armazenamento e back-up de dados pessoais

A Entrust utiliza múltiplos locais de servidor para armazenar e fazer back-up dos dados pessoais. Para locais de servidor utilizados por terceiros com os quais a Entrust se compromete a processar dados pessoais em nome de colegas e clientes, consulte as avaliações de impacto de proteção de dados relevantes referentes aos dados pessoais de colegas, bem como a página externa do subprocessador e avisos de privacidade de produtos para dados pessoais de clientes. Estes documentos estão localizados internamente, na página Compliance, ou externamente no site Jurídico e Compliance sob os ícones de Privacidade de dados. Para obter uma lista atual de locais de servidores de dados corporativos, os colegas também podem entrar em contato diretamente com o departamento de TI.

3.12 Transferências internacionais de dados e transferências para terceiros

Sob a GDPR, o Trust pode transferir dados pessoais para países fora do Espaço Econômico Europeu ("EEA") onde existe um nível adequado de proteção nesse país ou onde o Trust tenha adotado medidas apropriadas para garantir a proteção de dados.

As empresas dentro do grupo de confiança (ou seja, todas as entidades corporativas e subsidiárias) devem entrar no Acordo de Transferência de Dados Intra-Grupo a fim de garantir salvaguardas apropriadas para a transferência de dados pessoais fora da EEA, mas dentro do grupo de confiança.

Empresas fora do grupo Trust que processam dados pessoais para ou em nome do Trust, para as quais o Trust atua como controlador ou processador de dados, devem firmar um acordo de processamento de dados com o Trust para garantir salvaguardas apropriadas para a transferência de dados pessoais fora da EEA. Esse acordo contém linguagem para garantir que o terceiro tenha medidas técnicas e organizacionais apropriadas para cumprir com a GDPR e para assegurar a proteção dos direitos do sujeito dos dados.

Instâncias em que a Confiança transfere dados pessoais para um país fora da EEA pode incluir:

- O envolvido deu seu consentimento explícito à transferência proposta depois que a Confiança o informou de quaisquer possíveis riscos associados a tal transferência (por exemplo, a ausência, naquele país, de salvaguardas equivalentes);
- A transferência é necessária para a execução de um contrato no qual o envolvido é parte ou para tomar medidas a pedido do envolvido antes de firmar um contrato;
- A transferência é necessária para proteger os interesses vitais do envolvido ou de outra pessoa quando o envolvido for física ou legalmente incapaz de dar seu consentimento; ou
- A transferência é necessária para o estabelecimento ou defesa de uma reivindicação legal.

Para cada transferência de dados fora da AEA, a Confiança confiará nas Cláusulas Contratuais Padrão conforme definidas pela Comissão Européia (2001/497/CE, 2004/915/CE e 2010/87/UE).[1] Observe que um acordo de transferência de dados também é necessário se a transferência de dados pessoais for feita fora do Canadá.

3.13 Notificando os sujeitos dos dados

É necessário confiar o fornecimento de informações aos sujeitos dos dados sobre o processamento de seus dados pessoais. Estas informações estão contidas na Declaração de Privacidade da Empresa na Web que está disponível publicamente em www.entrust.com, na Declaração de Privacidade do Candidato a Emprego que está disponível publicamente em https://www.entrust.com/legal-compliance/data-privacy/job-applicant-privacy-statement, e na Declaração de Privacidade do Empregado que está disponível na intranet da Confiança. Tais declarações fornecem informações sobre:

- Os tipos de dados pessoais Processos de confiança;
- A finalidade e a base legal para o processamento de dados pessoais;
- Se os dados pessoais serão revelados a terceiros no decorrer do processamento;
- Se os dados pessoais serão transferidos para fora da AEA e do Canadá e, em caso afirmativo, que salvaguardas serão implementadas;
- Por quanto tempo os dados pessoais serão processados ou, se não for possível determinar, os critérios que a Empresa utilizará para determinar o período de processamento;
- Como o titular dos dados pode obter uma cópia de seus dados pessoais em poder da Confiança;
- Direitos do sujeito dos dados, incluindo como fazer uma reclamação;

[1] A partir de 27 de dezembro de 2022, essas transferências serão efetuadas utilizando as novas cláusulas contratuais padrão, conforme delineadas na Decisão de Implementação (UE) 2021/914 da Comissão, de 4 de junho de 2021, sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros, conforme o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

- Se os dados pessoais devem ser processados para cumprir uma lei ou um contrato, as possíveis conseqüências de o envolvido não fornecer os dados ou se opor ao processamento; e
- A existência e os detalhes de qualquer processo de decisão automatizado, quando aplicável.

Se o Entrust receber dados pessoais sobre um envolvido de terceiros, a Empresa também fornecerá ao envolvido informações sobre os mesmos:

- O tipo de dados pessoais recebidos do terceiro; e
- A fonte dos dados e se eles vieram de uma fonte acessível ao público (por exemplo, um website acessível ao público).

3.14 Avaliações de impacto de privacidade por projeto e proteção de dados

As leis de proteção de dados exigem que a Confiança considere a proteção de dados durante as etapas de desenvolvimento de uma nova oferta de produtos. A fim de satisfazer esta obrigação, o Trust deve tomar medidas para garantir que a proteção de dados faça parte do processo de projeto e que a coleta de dados pessoais seja minimizada na medida do possível.

Em algumas circunstâncias (nomeadamente, quando o processamento resultaria em alto risco para os direitos e liberdades de um indivíduo), pode ser necessário confiar na realização de uma avaliação formal do impacto da proteção de dados (DPIA) em relação ao processamento de dados pessoais. Tal avaliação envolve a documentação das finalidades para as quais a atividade é realizada, como a Confiança cumprirá as leis de proteção de dados e como a Empresa mitigará os riscos potenciais à privacidade dos indivíduos. Se você acredita que uma avaliação do impacto da proteção de dados pode ser necessária, entre em contato com o Diretor de Conformidade pelo e-mail privacy@entrust.com.

3.15 Direitos dos sujeitos dos dados

Se o encarregado processar dados pessoais, de acordo com as Leis de Proteção de Dados, o envolvido poderá ter o direito de:

- Solicitar informações sobre os dados pessoais mantidos com relação a eles;
- Ter quaisquer dados pessoais imprecisos sobre eles corrigidos e dados pessoais incompletos completados, sujeito à determinação de que os dados são, de fato, imprecisos ou incompletos;
- Objeto de confiar o processamento de seus dados pessoais quando a empresa o faz em busca de seus próprios interesses legítimos. A empresa pode continuar processando os dados pessoais não obstante uma objeção se os interesses legítimos da empresa superarem os da pessoa em questão, ou se a empresa precisar fazer isso para o estabelecimento ou defesa de uma reivindicação legal;
- Pedir à Trust para destruir os dados pessoais mantidos com respeito à pessoa em questão. A Empresa pode recusar este pedido se os dados pessoais ainda forem

necessários para os fins para os quais estão sendo processados e se houver uma base legítima para que a Confiança possa continuar o processamento;
- Solicite à Confiust que restrinja o processamento de seus dados pessoais ao armazenamento. Isto só pode ser solicitado se a exatidão dos dados pessoais tiver sido contestada e permanecer não verificada; a Entrust não requer mais os dados pessoais, mas o envolvido precisa deles para estabelecer ou defender uma reivindicação legal; o envolvido se opôs ao processamento de dados pessoais; e a Entrust está decidindo se seus interesses legítimos prevalecem sobre os interesses do envolvido ou se o processamento é ilegal.

A Entrust avaliará, caso a caso, os direitos do indivíduo dos dados, conforme a legislação aplicável sobre privacidade de dados para determinar como atender à solicitação de acesso do envolvido. De modo geral, a Entrust utilizará os direitos do envolvido sob a GDPR da UE como base para atender às solicitações e aplicar os direitos disponíveis sob a legislação aplicável de privacidade de dados na medida em que estes sejam mais favoráveis para o envolvido. Se um envolvido exercer estes direitos e a Entrust divulgar os dados pessoais em questão a um terceiro, a empresa fará o melhor para garantir que o terceiro também cumpra os desejos do envolvido.

3.16 Direitos de acesso aos dados

Os titulares dos dados que desejarem solicitar informações sobre os dados pessoais que a Confiança detém sobre eles podem fazê-lo enviando um Pedido de Acesso ao Assunto de Dados (DSAR) https://go.entrust.com/manage-db?_ga=2.102576711.793966578.1603810852-568122584.1603810852. Se os colegas receberem um pedido diretamente (seja verbalmente ou por escrito), encaminhe imediatamente os detalhes da solicitação para privacy@entrust.com. Para obter uma lista mais abrangente dos direitos individuais dos indivíduos dos dados por jurisdição, consulte o Procedimento de solicitação de acesso do detentor dos dados, disponível no site de Compliance.

3.17 Treinamento

Confiar a seus funcionários e trabalhadores contingentes o acesso a treinamento sobre as responsabilidades de proteção de dados. Este treinamento ocorre na integração e em intervalos regulares a partir daí.

3.18 Autoridades reguladoras

As informações de contato das autoridades reguladoras de dados relevantes variam de acordo com o local. Para obter a lista das autoridades do Conselho europeu de proteção de dados (European Data Protection Board), clique aqui. O Escritório do Comissário de Privacidade (Office of the Privacy Commissioner) do Canadá pode ser encontrado aqui.

3.19 Políticas de proteção de dados

Se você tiver dúvidas sobre o Sistema de Gerenciamento de Informações de Privacidade da Confiust, favor entrar em contato:

Entrust Corporation.

Atenção: Jenny Carmichael, Diretora de Conformidade

1187 Park Place

Shakopee, MN 55379

privacy@entrust.com

O responsável pela proteção de dados designado para a Entrust Deutschland GmbH é o Sr. Niels Kill da Althammer & Kill GmbH & Co. KG (kontakt-dsb@althammer-kill.de).

4. Conformidade

Espera-se que todos os funcionários e trabalhadores contingentes cumpram com esta política. Além disso, todas as unidades de negócios devem assegurar-se de ter padrões e procedimentos locais apropriados para cumprir esta política e a legislação aplicável de privacidade de dados em sua jurisdição. As violações desta política serão levadas a sério e podem resultar em ações disciplinares, até e incluindo a rescisão. Esta política pode ser atualizada ou emendada a qualquer momento.

5. Exceções

Não há exceções a esta política.

6. Propriedade e revisão

Esta política é de propriedade do Diretor Jurídico e de Conformidade. Esta política deve ser revista anualmente. As alterações neste documento deverão estar de acordo com o padrão de controle de documentos e registros do Sistema de Gerenciamento de Segurança da Informação (ISMS).

6.1 Informações de contato

Perguntas sobre esta política ou reclamações sobre o tratamento de dados pessoais devem ser dirigidas ao Diretor de Conformidade em privacy@entrust.com.

6.2 Propriedades de documentos e histórico de revisões

Propriedades do documento	
Propriedade	**Descrição**
Circulação	Uso interno e externo
Falsificação	Público
Proprietário do documento	Lisa Tibbits, Diretora Jurídica e de Conformidade
Próxima revisão programada	2022

Aprovações de documentos		
Nome do aprovador	**Título**	**Data**
Lisa Tibbits	Diretor Jurídico e de Conformidade	3-Mar-2019
Conselho de Governança Política	N/D	3-Ago-2021
Conselho de Governança Política	N/D	16-dez-2021

Histórico de revisão			
Versão	**Data**	**Descrição das mudanças**	**Revisado por**
1.0	19-Abr-2019	Versão inicial	Anjali Doherty, Sr. Tetina Corporativa; Jenny Carmichael, Diretora de Conformidade
1.1	19-Abr-2020	Atualizações anuais	Anjali Doherty, Sr. Tetina Corporativa; Jenny Carmichael, Diretora de Conformidade
1.2	10-Set-2020	Atualizado em novo modelo de política	Aileen Havel, Especialista Sênior em Conformidade
1.3	06-Jul-2021	Revisões anuais; seção adicional relativa ao acesso aos dados de categoria especial	Aileen Havel, advogada corporativa associada; Lee Jones, especialista sênior em Garantia de Conformidade
1.4	10-dez-2021	Atualizações para atender às recomendações de avaliação de risco externo e controles da ISO 27701	Jenny Carmichael, diretora de conformidade