POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS

Classificação	Público
Versão do documento	2.0
Data de publicação	26 de fevereiro de 2026

Índice

1. Introdução 4
2. Objetivo 4
3. Definições 4
4. Princípios fundamentais do tratamento de dados pessoais 5
5. Registros de Processamento 6
6. Legalidade e adequação 6
6.1 Bases legais para o tratamento de dados pessoais 6
6.2 Avaliações de privacidade 7
6.2.1 Avaliação de privacidade desde a concepção 7
6.2.2 Avaliação de impacto da proteção de dados (DPIA) 7
6.2.3 Avaliação de impacto da transferência de dados (DTIA) 7
6.2.4 Avaliação de impacto de interesse legítimo (LIIA) 7
6.2.5 Padrões de tratamento de dados confidenciais e de categorias especiais 8
6.2.6 Regra para Dados em Massa 8
6.3 Proteções contratuais 8
6.3.1 Contrato de transferência de dados intragrupo (IGDTA) 8
6.3.2 Contrato de tratamento de dados (DPA) 8
6.3.3 Disposições gerais de privacidade 9
7. Precisão e retenção 9
7.1 Gerenciamento de registros 9
7.2 Armazenamento e backup de dados pessoais 9
7.3 Apagamento ou destruição de dados pessoais 9
8. Confidencialidade e integridade 10
8.1 Segurança da Informação 10
8.2 Teste 11
8.3 Comunicação de incidente de dados pessoais 11
8.4 Resposta a incidentes com dados pessoais 12
9. Transparência 12
9.1 Avisos de privacidade 12
9.2 Treinamento 12
9.3 Direitos dos titulares dos dados 13
9.4 Autoridades reguladoras 14
9.5 Responsável pela proteção de dados 14

10. Conformidade 14
11. Exceções 14
12. Histórico de propriedade e revisão 14

1. Introdução

A Entrust Corporation e suas subsidiárias (coletivamente, "Entrust" ou a "Empresa") processam dados pessoais relacionados a nossos colegas e a contatos comerciais em nossos parceiros de vendas, fornecedores e clientes em nossa função de controladora de dados. A Entrust também processa dados pessoais relacionados aos funcionários e usuários finais de nossos clientes em nossa função como Processadora de Dados. Quando a Entrust processa dados pessoais, fazemos isso em conformidade com nossas obrigações legais e contratuais e com total transparência.

2. Objetivo

Esta política estabelece os requisitos e elementos do nosso programa global de privacidade de dados que a Entrust estabeleceu para garantir nossa conformidade com as obrigações legais e contratuais relevantes, bem como com os requisitos de certificação e auditoria. Esta política se aplica globalmente a todo o Processamento de dados pessoais realizado pela Entrust.

3. Definições

"Controladora de dados" significa a entidade que determina a finalidade e os meios de processamento de dados pessoais e tem o mesmo significado atribuído a 'Controladora de PII' de acordo com a ISO 27701.

"Processadora de dados" significa a entidade que processa dados pessoais em nome da controladora de dados e tem o mesmo significado atribuído a 'Processadora de PII' de acordo com a ISO 27701.

"Avaliação de impacto na proteção de dados" refere-se a uma análise documentada realizada por uma controladora ou processadora de dados que avalia os riscos de privacidade, em que o tratamento resultará, possivelmente, em um alto risco para os direitos e liberdades do titular dos dados.

"**Leis de proteção de dados**" refere-se a todas as leis e regulamentos de proteção de dados pessoais e privacidade aplicáveis à Entrust, incluindo, entre outros, o Regulamento geral de proteção de dados (GDPR) da União Europeia (UE), o Regulamento geral de proteção de dados do Reino Unido (UK GDPR), a Lei de Proteção de Dados de 2018 (DPA de 2018) do Reino Unido, a Lei federal de Proteção de Dados da Suíça (implementada em 1 de setembro de 2023) (FADP), a Lei de proteção de informações pessoais e documentos eletrônicos do Canadá (PIPEDA), a Lei de Proteção de Informações Pessoais (APPI) do Japão, a Lei de Proteção de Informações Pessoais (PIPL) da China e as leis estaduais de privacidade dos EUA, em cada caso, conforme alterações ou substituições.

"Titular dos dados" refere-se à pessoa identificada ou identificável ou ao domicílio a que os dados pessoais se referem e tem o mesmo significado atribuído a "Principal objeto de PII" da ISO 27701.

"Avaliação de impacto de transferência de dados" refere-se a uma análise documentada feita por uma controladora ou processadora de dados sobre o impacto e as implicações de segurança de

uma transferência de dados pessoais de dentro do Espaço Econômico Europeu (EEE) ou do Reino Unido (RU) para um país fora do EEE/Reino Unido que não tenha uma conclusão de adequação da Comissão Europeia ou do Gabinete do Comissário de Informações.

"Avaliação de impacto de interesse legítimo" refere-se à análise documentada realizada por um controlador ou processador de dados para averiguar se o interesse legítimo pode ser usado como base legal para o tratamento de dados pessoais. A avaliação inclui um teste de três passos que analisa se o tratamento de dados pessoais visa a um interesse legítimo, se é necessário para essa finalidade e se os interesses do titular dos dados prevalecem sobre o interesse legítimo.

"Dados pessoais" ou "PII" tem o significado atribuído a "informações de identificação pessoal", "informações pessoais" ou termos equivalentes, conforme definição nas leis de proteção de dados.

"Incidente com dados pessoais" tem o significado atribuído a "incidente de segurança", "violação de segurança" ou "violação de dados pessoais", ou termos equivalentes, conforme definição das leis de proteção de dados, e inclui qualquer situação em que a Entrust tome conhecimento de que os dados pessoais foram acessados, divulgados, alterados, perdidos, destruídos ou utilizados por pessoas não autorizadas, de forma não autorizada.

"Tratamento" refere-se a qualquer operação ou conjunto de operações que seja realizada com dados pessoais, seja 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 tratamento também inclui a transferência ou divulgação de dados pessoais a terceiros.

"Dados pessoais confidenciais" são um subconjunto de dados pessoais e referem-se a informações sobre um titular de dados que, se perdidas, comprometidas, acessadas ou divulgadas indevidamente, poderão resultar em danos, constrangimento, inconveniência ou injustiça para o titular dos dados e são portanto, sujeitos à proteção ampliada.

"Dados de Categoria Especial" é um subconjunto de dados pessoais e se refere a informações sobre a raça ou origem étnica de um indivíduo, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, e o Processamento de dados genéticos, dados biométricos para fins de identificação exclusiva de uma pessoa física, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa física.

4. Princípios fundamentais do tratamento de dados pessoais

A Entrust adere aos seguintes princípios fundamentais ao processar dados pessoais como uma controladora de dados:

- **Legalidade e adequação**: Garantimos que os dados pessoais sejam coletados para uma finalidade legal e limitados ao que é relevante e necessário para essa finalidade.

- **Precisão e retenção**: Mantemos nossos sistemas atualizados, fornecemos mecanismos para atualizar dados pessoais imprecisos e não retemos dados pessoais por mais tempo do que o necessário para cumprir a finalidade legal do processamento.
- **Confidencialidade e integridade**: Garantimos que os dados pessoais permaneçam seguros e protegidos durante o processamento, mas respondemos rápida e adequadamente a incidentes com dados pessoais, caso ocorram, inclusive fornecendo notificações oportunas, conforme necessário.
- **Justiça e Transparência**: Informamos os titulares dos dados quando tratamos os seus dados pessoais. Deixamos claro o motivo de precisarmos dos dados, como iremos usá-los e como serão tratados e protegidos. Fornecemos mecanismos para que os titulares dos dados exerçam os direitos a eles concedidos em relação aos seus dados pessoais, de acordo com a legislação aplicável.

Todos os colegas da Entrust são responsáveis por processar e proteger adequadamente os dados pessoais e entendem que a falha em fazê-lo tem o potencial não apenas de minar a confiança do cliente na Entrust, mas também de resultar em multas e penalidades significativas para a empresa.

5. Registros de Processamento

Para garantir a conformidade com as leis de proteção de dados aplicáveis e manter nosso compromisso com transparência e responsabilidade, a Entrust mantém um Registro de Atividades de Processamento (RoPA) de acordo com o Artigo 30 do GDPR e outras regulamentações de privacidade relevantes. O RoPA inclui todas as atividades de processamento que envolvem Dados Pessoais, conforme classificados de acordo com o Padrão de Classificação e Tratamento de Dados da Entrust.

6. Legalidade e adequação

6.1 Bases legais para o tratamento de dados pessoais

Ao atuar como Controladora de dados, a Empresa processa dados pessoais somente conforme legalmente permitido. A Entrust se baseia, acima de tudo, nas seguintes bases legais para tratamento:

- Assinatura de contrato;
- Cumprimento de obrigações legais, incluindo, entre outras, solicitações legais de autoridades policiais;
- Interesse legítimo, exceto quando tal interesse é anulado pelos interesses ou direitos e pelas liberdades fundamentais do envolvido; e
- Consentimento.

Quando o consentimento é a base legal para o processamento, a Entrust garante que o consentimento seja dado livremente, específico, informado e uma indicação inequívoca dos desejos do titular dos dados. O titular dos dados tem o direito de revogar o consentimento a qualquer momento e por qualquer motivo.

6.2 Avaliações de privacidade

6.2.1 Avaliação de privacidade desde a concepção

A Entrust avalia o Processamento de dados pessoais em relação aos princípios fundamentais descritos na Seção 4 acima como parte de seu projeto e desenvolvimento de ofertas de produtos novos ou substancialmente modificados e ao integrar soluções de fornecedores onde as PII serão processadas, incluindo licenciadas em aplicativos de software de terceiros. Essa avaliação "Privacy by Design" está incorporada nos processos de desenvolvimento e integração de fornecedores da Entrust. A conclusão da avaliação requer revisão e aprovação das equipes de privacidade e segurança da informação da Entrust. Não é possível dar continuidade ao desenvolvimento sem aprovação.

6.2.2 Avaliação de impacto da proteção de dados (DPIA)

Quando o tratamento de dados pessoais contemplado representa um alto risco para os direitos e liberdades de um indivíduo, a Entrust realiza uma DPIA para documentar e avaliar a finalidade do tratamento, como a Entrust cumprirá as leis de proteção de dados relevantes e como a Empresa mitigará riscos potenciais ao Titular dos Dados. Quando uma DPIA está relacionada ao Processamento em que a Entrust é a Controladora de Dados, ela é revisada pelo Diretor de Proteção de Dados da Entrust, que deve aprovar o Processamento proposto antes de seu início. As DPIAs devem ser revisadas e atualizadas pelo menos uma vez por ano, ou com maior frequência, conforme necessário, para garantir a conformidade contínua com as leis e regulamentações aplicáveis.

6.2.3 Avaliação de impacto da transferência de dados (DTIA)

Quando a Entrust pretende transferir dados pessoais de dentro do EEE ou do RU para um país fora do EEE ou do RU que não se beneficia de uma conclusão de adequação da Comissão Europeia ou do Gabinete do Comissário de Informações do RU, a Entrust preenche uma DTIA formal para analisar o impacto e as implicações de segurança da transferência, especialmente quando as leis do país receptor podem permitir o acesso do governo aos Dados Pessoais que estão sendo transferidos. A Entrust somente prosseguirá com a transferência quando concluir que o risco representado pela transferência é aceitável. Os DTIAs devem ser revistos e atualizados pelo menos anualmente, ou com maior frequência, se necessário, para garantir a conformidade contínua com as leis e regulamentos aplicáveis.

6.2.4 Avaliação de impacto de interesse legítimo (LIIA)

Quando a Entrust atua como controladora de dados e se baseia no interesse legítimo como base legal para o processamento de dados pessoais, a empresa conclui um LIIA formal para documentar e avaliar o interesse legítimo, determinar se o processamento é necessário e avaliar se os interesses, direitos e liberdades do titular dos dados superam ou se sobrepõem ao interesse legítimo. A Entrust somente prosseguirá com o Processamento com base no interesse legítimo quando o LIIA concluir que o interesse legítimo não é anulado.

6.2.5 Padrões de tratamento de dados confidenciais e de categorias especiais

Em sua função de Controladora de dados, a Entrust processa dados pessoais sensíveis relacionados a colegas em vários sistemas comerciais e alguns dados de categoria especial limitados de forma voluntária e conforme permitido pela legislação local. Os controles adequados estão em vigor e descritos nas DPIAs aplicáveis, no Padrão de Controle de Acesso para Dados de Categoria Especial e Sensível e no treinamento de privacidade aprimorado exigido para os colegas que lidam com esses Dados de Categoria Especial e Sensível.

6.2.6 Regra para Dados em Massa

Dados pessoais sensíveis, incluindo dados ômicos humanos, identificadores biométricos, dados de geolocalização precisos, dados pessoais de saúde, dados financeiros pessoais e determinados identificadores pessoais de cidadãos dos EUA, bem como dados do governo dos EUA, incluindo dados de geolocalização precisos para qualquer área especificamente designada, os quais apresentam um risco elevado de exploração (como instalações militares, segurança nacional, instalações de defesa ou inteligência, ou locais de trabalho de equipes de inteligência nacional federal), estão sujeitos a restrições de exportação, transferência e acesso. Esses dados não podem ser fornecidos a nenhuma pessoa ou entidade localizada, controlada ou agindo sob a direção de uma pessoa ou entidade localizada em um "país de preocupação". Atualmente, os "países de preocupação" são China (incluindo Hong Kong e Macau), Cuba, Irã, Coreia do Norte, Rússia e Venezuela.

Embora tal transferência ou acesso possa ser fornecido sob certas circunstâncias, a Entrust determinou que não se envolverá em nenhuma transação com países de preocupação que envolvam dados pessoais sensíveis dos EUA ou dados do governo dos EUA. Nenhum dado desse tipo deve ser transferido para um país de preocupação ou para uma pessoa ou entidade localizada em um país de preocupação, seja pela Entrust ou por qualquer pessoa agindo em nome da Entrust.

6.3 Proteções contratuais

6.3.1 Contrato de transferência de dados intragrupo (IGDTA)

A Entrust Corporation e suas subsidiárias celebram o Contrato de transferência de dados intragrupo para garantir que, quando os dados pessoais forem compartilhados dentro do grupo Entrust, isso seja coberto por cláusulas de compartilhamento de dados apropriadas (incluindo cláusulas de controlador - processador, conforme exigido pelo RGPD). O IGDTA também garante que existam salvaguardas adequadas (ou seja, cláusulas contratuais padrão) para quando o compartilhamento de dados pessoais dentro do grupo Entrust envolver a transferência de dados pessoais de dentro do EEE/Reino Unido para um país fora do EEE/Reino Unido que não se beneficia de uma conclusão de adequação da Comissão Europeia ou do Gabinete do Comissário de Informação.

6.3.2 Contrato de tratamento de dados (DPA)

As empresas fora do grupo Entrust que tratam dados pessoais para ou em nome da Entrust são obrigadas a celebrar um Contrato de tratamento de dados com a Entrust para garantir que o terceiro (por exemplo, vendedor, fornecedor, parceiro de canal) tenha medidas técnicas e organizacionais apropriadas em vigor para cumprir as leis de proteção de dados relevantes. A Entrust assume

compromissos equivalentes com seus clientes quando atua como Processadora de Dados através de um DPA padrão do cliente.

6.3.3 Disposições gerais de privacidade

A redação contratual em torno da privacidade também está incorporada em acordos padrão com clientes, fornecedores e parceiros, bem como no Acordo de não divulgação (NDA) padrão da Entrust. Contratos com fornecedores também incluem obrigações de conformidade com a Regra para Dados em Massa.

7. Precisão e retenção

7.1 Gerenciamento de registros

O programa global de Gerenciamento de registros garante que um período de retenção seja formalmente definido para o tratamento de dados pessoais, para garantir que sejam mantidos apenas pelo tempo necessário e que os dados pessoais sejam apagados, destruídos ou mantidos anonimizados no final do período de retenção atribuído. A Política global de gerenciamento de registros estabelece requisitos de tratamento para todos os registros, não apenas para aqueles que contêm dados pessoais, e o Cronograma de retenção de registros que a acompanha define o período de retenção para cada tipo de registro mantido pela Empresa.

7.2 Armazenamento e backup de dados pessoais

A Entrust armazena e faz backup de dados pessoais em vários locais de servidores gerenciados direta e indiretamente pela Empresa. O setor de TI e os fornecedores relevantes (para aplicativos não gerenciados pela TI e hospedados na nuvem) recebem orientações padrão sobre o manuseio adequado de dados pessoais nesses servidores, inclusive com relação ao armazenamento e backups. A Entrust não remove cópias de dados pessoais de suas mídias e servidores de backup no final do período de retenção quando tal conduta seria comercialmente impraticável; no entanto, os dados pessoais retidos pela Entrust desta forma são protegidos pelos mesmos padrões de segurança que protegem os dados pessoais durante o uso, e os dados pessoais permanecem sujeitos à confidencialidade e não podem ser acessados, exceto conforme exigido pela lei aplicável.

7.3 Apagamento ou destruição de dados pessoais

A Política global de gerenciamento de registros e o Padrão de tratamento e classificação de dados estabelecem os requisitos para o tratamento adequado de registros de todos os tipos no final do período de retenção prescrito. Em particular, os seguintes princípios aplicam-se no que diz respeito aos registros que contêm dados pessoais:

- Os dados pessoais não devem ser copiados, exceto quando necessário para cumprir a finalidade especificada de tratamento, e toda cópia feita deve reter as marcas originais de confidencialidade ou propriedade.
- Os registros físicos devem ser triturados e descartados de forma segura quando não houver mais necessidade de mantê-los e não poderão ser descartados de qualquer outra maneira.
- Os dados pessoais em formato eletrônico devem ser excluídos ou mantidos anonimizados quando já não forem necessários.

- O setor de TI é responsável por destruir ou apagar equipamentos eletrônicos que contenham dados pessoais (por exemplo, laptops, desktops, dispositivos móveis de propriedade da empresa e dados de trabalho em dispositivos do tipo "Traga seu próprio dispositivo (BYOD)") de acordo com as políticas e padrões relevantes de segurança da informação.

8. Confidencialidade e integridade

8.1 Segurança da Informação

Quando a Empresa trata dados pessoais, ela toma medidas razoáveis para garantir que os dados permaneçam seguros e protegidos contra tratamento não autorizado ou ilegal, perda acidental, destruição ou danos. A Entrust faz isso das seguintes formas:

- Criptografando dados pessoais em repouso e em trânsito, quando exigido por lei ou contrato, e de forma complementar, conforme comercialmente praticável;
- Garantindo a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços utilizados para tratar dados pessoais por planos formalizados de recuperação de negócios e de recuperação de desastres que são rotineiramente testados ou praticados;
- Garantindo a restauração do acesso aos dados pessoais em tempo hábil em caso de incidente físico ou técnico;
- Testando e avaliando periodicamente a eficácia das medidas técnicas e organizacionais implementadas para proteger os dados pessoais;
- Colocando em vigor padrões de segurança física que exigem que mesas e armários fiquem trancados se contiverem dados pessoais, monitores/telas individuais não deixem visíveis dados pessoais aos transeuntes e dispositivos eletrônicos (por exemplo, computadores, tablets) fiquem bloqueados ou desconectados dos sistemas da Empresa quando deixados sem supervisão.

Ao avaliar os controles de segurança apropriados, a Entrust considera os riscos associados ao tratamento, em particular os riscos de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos dados pessoais que são processados.

Quando a Entrust contrata terceiros para tratar dados pessoais em seu nome, essas partes o fazem com base em instruções escritas da Entrust e sujeitas a disposições contratuais (por exemplo, DPA) para tratar adequadamente os dados pessoais e implementar medidas técnicas e organizacionais apropriadas que sejam pelo menos equivalentes aos próprios requisitos de segurança da Entrust. Os dados pessoais não são compartilhados fora da Entrust sem a implementação desses mecanismos. Várias ferramentas de segurança (por exemplo, DLP) estão em vigor para garantir que os dados pessoais não saiam da organização sem autorização.

8.2 Teste

Os dados pessoais não podem ser usados em nenhum ambiente de teste da Entrust sem uma exceção de segurança formal aprovada antecipadamente. Todos os ambientes de teste devem aderir aos padrões e controles atuais em vigor para ambientes de produção e todos os dados pessoais aprovados para uso em ambientes de teste devem ser removidos sem demora após a conclusão do teste. Mais detalhes estão descritos no Ciclo de Vida de Desenvolvimento de Software Seguro (S-SDLC).

8.3 Comunicação de incidente de dados pessoais

Um incidente de dados pessoais pode assumir muitas formas, incluindo, entre outras:

- Perda de dispositivo móvel ou arquivo de cópia impressa contendo dados pessoais (por exemplo, deixar acidentalmente um dispositivo no transporte público);
- Roubo de dispositivo móvel ou arquivo impresso contendo dados pessoais;
- Erro humano (por exemplo, um colega envia acidentalmente um e-mail contendo dados pessoais para um destinatário não intencional, ou altera ou apaga 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 da Entrust);
- Perda e destruição física (por exemplo, incêndio ou inundação); ou
- Obtenção de informações com a Entrust por terceiros por meio de fraude (por exemplo, ataques de phishing ou smishing).

Um incidente de dados pessoais pode ter ocorrido em caso de:

- Login incomum e/ou atividade excessiva do sistema 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 Entrust;
- Falha de equipamento; ou
- Registradores de chaves de hardware ou software conectados ou instalados em sistemas da Entrust.

Os colaboradores que tomarem conhecimento ou tiverem qualquer motivo para suspeitar que um incidente com dados pessoais pode ter ocorrido, ou está prestes a ocorrer, devem entrar em contato imediatamente com o Centro de Operações de Segurança da Entrust pelo e-mail SOC@entrust.com.

8.4 Resposta a incidentes com dados pessoais

No caso de incidente, real ou iminente, com dados pessoais, a Entrust implementará seus procedimentos de resposta e tratamento de incidentes mantidos pela equipe de Segurança da Informação para minimizar o impacto do incidente e notificar reguladores, titulares de dados e/ou outras partes conforme exigido por lei e/ou contrato. Normalmente, a resposta envolve o seguinte:

- Investigar o incidente para determinar a natureza, causa e extensão dos danos ou prejuízos causados ou 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 obrigação de notificar outras partes (por exemplo, autoridades nacionais de proteção de dados, pessoas afetadas, partes previstas em contrato) e fazer essas notificações em tempo hábil; e
- Registrar informações sobre o incidente de dados pessoais e as medidas tomadas em resposta, inclusive documentando decisões de notificar ou não os reguladores ou as partes afetadas.

9. Transparência

A Entrust garante a transparência em relação ao seu programa global de privacidade de dados utilizando páginas internas e externas robustas.

9.1 Avisos de privacidade

A Entrust notifica os titulares dos dados sobre o tratamento de seus dados pessoais em sua função de controladora e processadora de dados. Essas informações estão disponíveis em vários avisos de privacidade da Entrust para usuários da Web, candidatos a empregos e colaboradores, bem como em avisos de privacidade de produtos individuais, disponíveis aqui. Tais avisos fornecem informações sobre:

- Os tipos de processos de dados pessoais da Entrust;
- A finalidade e a base legal do tratamento;
- Terceiros envolvidos no tratamento, se aplicável;
- Local e duração do tratamento;
- Transferências transfronteiriças de dados pessoais;
- Duração do tratamento;
- Direitos do titular dos dados; e
- Detalhes sobre processos de tomada de decisão automatizados/por inteligência artificial

9.2 Treinamento

A Entrust oferece aos colaboradores treinamento anual obrigatório sobre responsabilidades de proteção de dados. O Treinamento de introdução à privacidade de dados ocorre na integração e, a

partir de então, uma vez ao ano. Além do Treinamento de introdução à privacidade de dados para todos os colaboradores, a Entrust exige a realização anual do Treinamento avançado de privacidade de dados por colaboradores que lidam com dados confidenciais e de categorias especiais, bem como o Treinamento de privacidade desde a concepção por colaboradores que desempenham função no desenvolvimento e concepção de ofertas de produtos e serviços de software. A Entrust continua a desenvolver e implantar treinamentos de privacidade específicos de funções adicionais, conforme necessário.

9.3 Direitos dos titulares dos dados

Quando a Entrust trata dados pessoais, as leis de proteção de dados estabelecem determinados direitos aos titulares dos dados. Embora estes direitos variem de acordo com a localidade, no geral, os titulares dos dados têm o direito de:

- Solicitar informações sobre os dados pessoais que a Entrust mantém sobre eles, incluindo uma cópia dessas informações;
- Ter quaisquer dados pessoais imprecisos sobre eles corrigidos e dados pessoais incompletos complementados;
- Opor-se ao tratamento de seus dados pessoais pela Entrust quando a Empresa o fizer em defesa de seus próprios interesses legítimos. A Entrust pode continuar tratando os dados pessoais não obstante objeção se os interesses legítimos da Empresa superarem os da pessoa em questão, ou se a Entrust precisar fazer isso por questões legais;
- Pedir à Entrust para destruir os dados pessoais mantidos com respeito ao titular dos dados. A Empresa pode recusar este pedido se os dados pessoais ainda forem necessários para os fins para os quais estão sendo tratados e se houver uma base legal para que a Entrust possa continuar o tratamento;
- Pedir à Entrust para restringir o tratamento de seus dados pessoais ao armazenamento sob determinadas circunstâncias.

A Entrust avaliará caso a caso os direitos do titular dos dados de acordo com as leis de proteção de dados e seguirá o Procedimento de solicitação do titular dos dados (DSR) para determinar como atender a uma solicitação. De modo geral, a Entrust utilizará os direitos do titular dos dados previstos pelo GDPR da UE como base para atender a todas as solicitações e aplicar direitos adicionais disponíveis sob as leis de proteção de dados que se aplicam ao titular dos dados na medida em que estes sejam mais favoráveis ao envolvido. Se um titular de dados exercer esses direitos e a Entrust divulgar os dados pessoais em questão a um terceiro, a Empresa envidará seus melhores esforços para garantir que o terceiro também cumpra os desejos do titular dos dados.

Os titulares dos dados que desejarem solicitar informações sobre os dados pessoais que a Entrust detém sobre eles podem fazê-lo por meio de envio de uma Solicitação do titular dos dados (DSR) formal. Se os colaboradores receberem uma solicitação diretamente (verbal ou por escrito), a solicitação deverá ser encaminhada imediatamente para privacy@entrust.com.

9.4 Autoridades reguladoras

As informações de contato das autoridades reguladoras de dados relevantes variam de acordo com o local. A lista de autoridades do Conselho Europeu de Proteção de Dados pode ser encontrada aqui. O Gabinete do Comissário de Informações do Reino Unido (Information Commissioner's Office, ICO) pode ser encontrado aqui. O Gabinete do Comissário de Privacidade do Canadá pode ser encontrado aqui.

9.5 Responsável pela proteção de dados

Salvo indicação em contrário, o Responsável pela Proteção de Dados da Entrust é:

Mishcon de Reya LLP
Africa House, 70 Kingsway, London, WC2B 6AH, Reino Unido
DPO@mishcon.com

10. Conformidade

Espera-se que todos os colaboradores e trabalhadores temporários cumpram 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 localidade. As violações desta política serão levadas a sério e podem resultar em medidas disciplinares, inclusive rescisão. Esta política pode ser atualizada ou alterada a qualquer momento.

11. Exceções

Não há exceções a esta política.

12. Histórico de propriedade e revisão

Esta Política é detida pela Diretor de Privacidade e deve ser revista anualmente.