POLÍTICA GLOBAL DE PROTECCIÓN DE DATOS PERSONALES

Clasificación	Público
Versión del documento	2.0
Fecha de publicación	26 de febrero de 2026

Contenido

1. Introducción

Entrust Corporation y sus subsidiarias (en conjunto, "Entrust" o la "Empresa") procesan Datos personales pertenecientes a nuestros colegas y contactos comerciales en nuestros socios de ventas, proveedores y clientes en nuestro papel como controlador de datos. Entrust también procesa Datos personales relativos a los empleados y usuarios finales de nuestros clientes en nuestro papel de Procesador de datos. Cuando Entrust procesa Datos personales, lo hace en cumplimiento de sus obligaciones legales y contractuales y con total transparencia.

2. Propósito

Esta política establece los requisitos y elementos de nuestro programa global de privacidad de datos que Entrust ha establecido para garantizar que cumplimos las obligaciones legales y contractuales pertinentes, así como los requisitos de certificación y auditoría. Esta política se aplica globalmente a todo el procesamiento de Datos Personales realizado por Entrust.

3. Definiciones

"Controlador de datos" es la entidad que determina la finalidad y los medios del Procesamiento de Datos personales y tiene el mismo significado atribuido a "Controlador de la información de identificación personal" en la norma ISO 27701.

"Procesador de datos" es la entidad que procesa los Datos personales en representación del controlador de datos y tiene el mismo significado atribuido a "Controlador de la información de identificación personal" en la norma ISO 27701.

"Evaluación de impacto relativa a la protección de datos" se refiere a un análisis documentado realizado por un controlador o procesador de datos en el que se evalúan los riesgos para la privacidad cuando es probable que el procesamiento suponga un alto riesgo para los derechos y libertades del interesado.

"Leyes de protección de datos" hace referencia a todas las leyes y normativas de protección de Datos personales y privacidad aplicables a Entrust, incluidas, entre otras, el Reglamento General de Protección de Datos (GDPR) de la UE, el Reglamento General de Protección de Datos del Reino Unido (GDPR del RU), Ley de Protección de Datos del Reino Unido (DPA 2018), Ley Federal Suiza de Protección de Datos (implementada el 1 de septiembre de 2023) (FADP), la Ley de Protección de la Información Personal y los Documentos Electrónicos de Canadá (LPRPDE), Ley de Protección de Información Personal de Japón (APPI), Ley de Protección de Información Personal de China (PIPL) y las leyes de privacidad de los estados de EE. UU., en cada caso en su versión modificada, sustituida o reemplazada.

"Sujeto de los datos" es la persona identificada o identificable o el hogar al que se refieren los Datos personales y tiene el mismo significado atribuido a "Principal de información de identificación personal" según la norma ISO 27701.

"Evaluación del impacto de la transferencia de datos" se refiere a un análisis documentado realizado por un controlador o procesador de datos del impacto y las implicaciones de seguridad de una transferencia de Datos personales a un país dentro del Espacio Económico Europeo o el Reino Unido a un país fuera del Espacio Económico Europeo/Reino Unido que no tiene una conclusión de adecuación por parte de la Comisión Europea o la Oficina del Comisionado de Información.

"Evaluación del impacto del interés legítimo" se refiere a un análisis documentado realizado por controlador o procesador de datos sobre si el interés legítimo puede utilizarse como base jurídica para el Procesamiento de Datos personales. La evaluación incluye una triple prueba que analiza si el procesamiento de Datos personales persigue un interés legítimo, si es necesario para ese fin y si los intereses del interesado prevalecen sobre el interés legítimo.

"Datos personales" o "PII" tiene el significado atribuido a "información de identificación personal", "información personal" o términos equivalentes según se definen en las leyes de protección de datos.

"Incidente de datos personales" tiene el significado atribuido a "incidente de seguridad", "violación de seguridad" o "violación de Datos personales" o términos equivalentes, tal y como se definen dichos términos en la legislación de protección de datos, e incluye cualquier situación en la que Entrust tenga conocimiento de que se ha accedido, revelado, alterado, perdido, destruido o utilizado Datos personales por personas no autorizadas, de forma no autorizada.

"Procesamiento" se refiere a cualquier operación o conjunto de operaciones que se realiza con los Datos personales, ya sea por medios automáticos o no, como la recopilación, registro, estructura de la organización, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o de otra manera que los haga disponibles, alineación o combinación, restricción, borrado o destrucción. El procesamiento también incluye la transferencia o divulgación de Datos personales a terceros.

"Datos personales sensibles" es un subconjunto de los Datos personales y se refiere a la información sobre un interesado que, si se pierde, se pone en peligro, se accede a ella o se divulga indebidamente, podría resultar perjudicial, embarazosa, inconveniente o injusta para el interesado y, por lo tanto, está sujeta a una mayor protección.

"Datos de categoría especial" es un subconjunto de los Datos personales y se refiere a la información sobre la raza o el origen étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical de una persona, así como al procesamiento de datos genéticos y datos biométricos con el fin de identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física.

4. Principios básicos del tratamiento de datos personales

Entrust se adhiere a los siguientes principios fundamentales cuando procesa Datos personales como Controlador de datos:

- **Legalidad y adecuación**: Nos aseguramos de que los Datos personales se recojan con un fin lícito y se limiten a los que sean pertinentes y necesarios para dicho fin.
- **Precisión y retención**: Mantenemos nuestros sistemas actualizados, proporcionamos mecanismos para actualizar o eliminar los Datos personales inexactos y no conservamos los Datos personales más tiempo del necesario para cumplir la finalidad legal del Procesamiento.
- **Confidencialidad e integridad**: Garantizamos que los Datos personales permanezcan seguros y protegidos durante el Procesamiento, pero respondemos rápida y adecuadamente a los incidentes con Datos personales si ocurren, incluida la notificación oportuna según sea necesario.
- **Equidad y transparencia**: Informamos adecuadamente a los interesados cuando procesamos sus Datos personales. Tenemos claro por qué los necesitamos, cómo los utilizaremos y cómo se tratarán y protegerán. Proporcionamos mecanismos para que los interesados ejerzan los derechos que tienen con respecto a sus Datos personales en virtud de la legislación aplicable.

Todos los colegas de Entrust son responsables de procesar y salvaguardar adecuadamente los Datos personales y comprendemos que no hacerlo puede no solo socavar la confianza de los clientes en Entrust, sino dar lugar a multas y sanciones significativas para la empresa.

5. Registros de procesamiento

Para garantizar el cumplimiento de las leyes de protección de datos aplicables y mantener nuestro compromiso con la transparencia y la responsabilidad, Entrust mantiene un Registro de Actividades de Procesamiento (RoPA) de conformidad con el artículo 30 del GDPR y otras normas de privacidad pertinentes. La RoPA incluye todas las actividades de procesamiento que implican Datos personales clasificados de acuerdo con la Norma de Clasificación y Tratamiento de Datos de Entrust.

6. Legalidad y adecuación

6.1 Bases jurídicas para el procesamiento de datos personales

Cuando actúa como Controlador de datos, la Empresa solo procesa Datos personales según lo permitido legalmente. Entrust se basa principalmente en las siguientes bases legales para el Procesamiento:

- Ejecución de un contrato;
- Cumplimiento de obligaciones legales, incluidas, entre otras, las solicitudes legales de las fuerzas y cuerpos de seguridad;

- Intereses legítimos, excepto cuando dichos intereses prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado; y
- Consentimiento.

Cuando el consentimiento es la base jurídica para el Procesamiento, Entrust garantiza que el consentimiento se da libremente, es específico e informado y constituye una indicación inequívoca de los deseos del interesado. El interesado tiene derecho a retirar su consentimiento en cualquier momento y por cualquier motivo.

6.2 Evaluaciones de privacidad

6.2.1 Evaluación de privacidad por diseño

Entrust evalúa el Procesamiento de Datos personales con respecto a los principios básicos descritos en la Sección 4 anterior como parte de su diseño y desarrollo de ofertas de productos nuevos o modificados sustancialmente y al incorporar soluciones alojadas en la nube de proveedores donde se procesarán PII, incluidas las aplicaciones de software de terceros con licencia. Esta evaluación de "Privacidad por diseño" está integrada en los procesos de desarrollo e incorporación de proveedores de Entrust. La finalización de la evaluación requiere la revisión y aprobación de los equipos de Privacidad y Seguridad de la Información de Entrust. El desarrollo no puede avanzar sin aprobación.

6.2.2 Evaluación de impacto de la protección de datos (DPIA)

Cuando el Procesamiento de Datos personales contemplado plantea un alto riesgo para los derechos y libertades de una persona, Entrust completa una DPIA formal para documentar y evaluar el propósito del Procesamiento, cómo cumplirá Entrust con las Leyes de Protección de Datos pertinentes y cómo mitigará la empresa los riesgos potenciales para los derechos de los interesados. Cuando una DPIA se relaciona con un Procesamiento posterior en el que Entrust es el Controlador de datos, es revisada por el Responsable de Protección de datos de Entrust, que debe aprobar el Procesamiento posterior propuesto antes de que comience. Las DPIA se revisarán y actualizarán al menos una vez al año, o con mayor frecuencia si fuera necesario, para garantizar el cumplimiento continuado de las leyes y reglamentos aplicables.

6.2.3 Evaluación del impacto de la transferencia de datos (DTIA)

Cuando Entrust tiene la intención de transferir Datos personales desde un país dentro del Espacio Económico Europeo (EEE) o el Reino Unido (RU) a un país fuera del Espacio Económico Europeo (EEE) o el Reino Unido (RU) que no se beneficia de una decisión de adecuación de la Comisión Europea o la Oficina del Comisionado de Información del Reino Unido, Entrust completa un DTIA formal para analizar el impacto y las implicaciones de seguridad de la transferencia, en particular cuando las leyes del país receptor podrían permitir a su gobierno el acceso a los Datos personales que se transfieren. Entrust solo procederá a la transferencia cuando llegue a la conclusión de que el riesgo que plantea la transferencia es aceptable. Las DTIA se revisarán y actualizarán al menos una vez al año, o con mayor frecuencia según sea necesario, para garantizar el cumplimiento continuo de las leyes y regulaciones aplicables.

6.2.4 Evaluación del impacto del interés legítimo (LIIA)

Cuando Entrust actúa como Controlador de datos se basa en el interés legítimo como fundamento jurídico para el Procesamiento de Datos personales, la empresa completa una LIIA formal para documentar y evaluar el interés legítimo, determinar si el Procesamiento es necesario y evaluar si los intereses, derechos y libertades del Sujeto de datos prevalecen sobre el interés legítimo. Entrust solo procederá al Procesamiento posterior sobre la base del interés legítimo cuando la LIIA concluya que el interés legítimo no queda anulado.

6.2.5 Normas para el tratamiento de datos sensibles y de categoría especial

En su papel de Controlador de datos, Entrust procesa Datos personales sensible en nombre de colegas a través de varios sistemas empresariales y algunos Datos limitados de Categoría especial de forma voluntaria y según lo permita la legislación local. Se han establecido los controles adecuados, que se describen en las evaluaciones de impacto sobre la protección de datos aplicables, en la norma de control de acceso a datos sensibles y de categoría especial y en la formación reforzada en materia de protección de la intimidad que se exige a los colegas que manejan estos datos sensibles y de categoría especial.

6.2.6 Regla de datos masivos

Los datos personales sensibles, incluidos los datos ómicos humanos, los identificadores biométricos, los datos de geolocalización precisos, los datos sanitarios personales, los datos financieros personales y determinados identificadores personales de ciudadanos estadounidenses, así como los datos gubernamentales estadounidenses, incluidos los datos de geolocalización precisos de cualquier zona designada específicamente como de alto riesgo de explotación (como instalaciones militares, instalaciones de seguridad nacional, defensa o inteligencia, o lugares de trabajo de personal de inteligencia nacional federal) están sujetos a restricciones de exportación, transferencia y acceso. Estos datos no pueden proporcionarse a ninguna persona o entidad ubicada en, controlada por, o que actúe bajo la dirección de una persona o entidad ubicada en un "país de preocupación". Actualmente, los "países de preocupación" son China (incluidos Hong Kong y Macao), Cuba, Irán, Corea del Norte, Rusia y Venezuela.

Aunque dicha transferencia o acceso puede proporcionarse en determinadas circunstancias, Entrust ha determinado que no participará en ninguna transacción con países de preocupación que implique datos personales sensibles de Estados Unidos o datos gubernamentales de Estados Unidos. Ni Entrust ni nadie que actúe en nombre de Entrust debe transferir nunca dichos datos a un país de preocupación o a una persona o entidad ubicada en un país de preocupación.

6.3 Protecciones contractuales

6.3.1 Acuerdo de transferencia de datos intragrupo (IGDTA)

Entrust Corporation y sus filiales celebran el Acuerdo de Transferencia de Datos Intragrupo para garantizar que cuando se compartan Datos personales dentro del grupo Entrust, esto esté cubierto por las cláusulas adecuadas de intercambio de datos (incluidas las cláusulas controlador - procesador según lo requerido por el GDPR). La IGDTA también garantiza la existencia de

salvaguardias adecuadas (es decir, cláusulas contractuales estándar) para cuando el intercambio de Datos personales dentro del grupo Entrust implique la transferencia de Datos personales desde dentro del EEE/Reino Unido a un país fuera del EEE/Reino Unido que no se beneficie de una decisión de adecuación de la Comisión Europea o de la Oficina del Comisionado de Información.

6.3.2 Acuerdo de procesamiento de datos (DPA)

Las empresas ajenas al grupo Entrust que procesan Datos personales para o en representación de Entrust están obligadas a firmar un Acuerdo de Procesamiento de Datos con Entrust para garantizar que el tercero (por ejemplo, vendedor, proveedor, socio de canal) cuenta con las medidas técnicas y organizativas adecuadas para cumplir con las leyes de protección de datos pertinentes. Entrust asume compromisos equivalentes con sus clientes cuando actúa como Procesador de datos a través de un APD estándar del cliente.

6.3.3 Disposiciones generales sobre privacidad

El lenguaje contractual en torno a la privacidad también se incluye en los acuerdos estándar con clientes, proveedores y socios, así como en el acuerdo de confidencialidad estándar de Entrust. Los contratos con vendedores y proveedores también incluyen la obligación de cumplir la Regla de Datos Masivos.

7. Precisión y retención

7.1 Gestión de registros

El programa global de gestión de registros garantiza que se defina formalmente un periodo de conservación para el Procesamiento de los Datos personales, a fin de garantizar que solo se conserven durante el tiempo necesario, y que los Datos personales se borren, destruyan o anonimicen al final del periodo de conservación asignado. La política global de gestión de registros establece los requisitos de gestión de todos los registros, no sólo los que contienen Datos personales, y el calendario de conservación de registros define el periodo de conservación para cada tipo de registro conservado por la Empresa.

7.2 Almacenamiento y copias de seguridad de datos personales

Entrust almacena y realiza copias de seguridad de los Datos personales en múltiples ubicaciones de servidores gestionados directa e indirectamente por la empresa. TI y los proveedores pertinentes (para aplicaciones alojadas en la nube y no gestionadas por TI) reciben orientaciones estándar sobre el tratamiento adecuado de los Datos personales en estos servidores, incluso con respecto al almacenamiento y las copias de seguridad.

Entrust no elimina las copias de Datos personales de sus soportes y servidores de copia de seguridad al final del período de conservación cuando hacerlo sería comercialmente impracticable; sin embargo, los Datos personales conservados por Entrust de esta manera están protegidos por las mismas normas de seguridad que protegen los Datos personales mientras están en uso y los Datos personales siguen estando sujetos a confidencialidad y no se puede acceder a ellos excepto cuando lo exija la legislación aplicable.

7.3 Borrado o destrucción de datos personales

La Política Global de Gestión de Registros y la Norma de Tratamiento de la Clasificación de los Datos establecen los requisitos para el tratamiento adecuado de los registros de todo tipo al final de su periodo de conservación prescrito. En particular, se aplican los siguientes principios con respecto a los registros que contienen Datos personales:

- Los Datos personales no deben copiarse, salvo en la medida en que sea necesario para cumplir la finalidad especificada del Procesamiento, y las copias que se hagan deben conservar las marcas originales de confidencialidad o propiedad.
- Los registros en papel deben triturarse y eliminarse de forma segura cuando ya no sea necesario conservarlos, y no pueden eliminarse de ninguna otra forma.
- Los Datos personales en formato electrónico deben eliminarse o anonimizarse cuando ya no sean necesarios.
- TI es responsable de destruir o borrar los equipos electrónicos que contengan Datos personales (por ejemplo, computadoras portátiles, computadoras de escritorio, dispositivos móviles propiedad de la empresa y datos de trabajo en dispositivos Bring Your Own Device (BYOD)) de acuerdo con las políticas y normas pertinentes de Seguridad de la Información.

8. Confidencialidad e integridad

8.1 Seguridad de la información

Cuando la Empresa procesa Datos personales, toma medidas razonables para garantizar que los Datos personales permanezcan seguros y estén protegidos contra el Procesamiento no autorizado o ilegal, la pérdida accidental, la destrucción o el daño. Entrust hace esto mediante lo siguiente:

- Cifrar los Datos personales en reposo y en tránsito cuando lo exija la ley o un contrato y, además, en la medida en que sea comercialmente viable;
- Garantizar la confidencialidad, integridad, disponibilidad y resistencia permanentes de los sistemas y servicios utilizados para procesar Datos personales mediante planes formalizados de recuperación de la actividad y de recuperación en caso de catástrofe que se comprueben o ejerciten de forma rutinaria;
- La garantía del restablecimiento del acceso a los Datos personales de manera oportuna en caso de un incidente físico o técnico;
- Comprobar, valorar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas adoptadas para proteger los Datos personales;
- Aplicar normas de seguridad física que exigen que los escritorios y armarios se mantengan cerrados con llave si contienen Datos personales, que los monitores/pantallas individuales no permitan que los Datos personales sean visibles para los transeúntes y que los dispositivos electrónicos (por ejemplo, computadoras, tabletas) se bloqueen o se desconecten de los sistemas de la empresa cuando se dejan desatendidos.

Al evaluar los controles de seguridad adecuados, Entrust tiene en cuenta los riesgos asociados con el Procesamiento, en particular los riesgos de destrucción accidental o ilícita, pérdida, alteración, divulgación no autorizada de los Datos personales tratados o acceso a ellos.

Cuando Entrust contrata a terceros para procesar Datos personales en su representación, dichos terceros lo hacen basándose en instrucciones escritas de Entrust y sujetos a disposiciones contractuales (por ejemplo, DPA) para manejar adecuadamente los Datos personales e implementar medidas técnicas y organizativas apropiadas que sean al menos equivalentes a los propios requisitos de seguridad de Entrust. Los Datos personales no se comparten fuera de Entrust sin que existan estos mecanismos. Existen varias herramientas de seguridad (por ejemplo, DLP) para garantizar que los Datos personales no salgan de la organización sin autorización.

8.2 Pruebas

Los Datos personales no podrán utilizarse en ningún entorno de pruebas de Entrust sin una excepción de seguridad formal aprobada de antemano. Todos los entornos de prueba deben cumplir las normas y controles vigentes para los entornos de producción, y todos los Datos personales aprobados para su uso en entornos de prueba deben eliminarse sin demora una vez finalizadas las pruebas. Puede obtener más detalles en el Ciclo de vida de desarrollo de software seguro (S-SDLC).

8.3 Informar un incidente relacionado con datos personales

Un incidente relacionado con Datos personales puede adoptar muchas formas, entre ellas:

- Pérdida de un dispositivo móvil o de un archivo impreso que contenga Datos personales (por ejemplo, dejar accidentalmente un dispositivo en el transporte público).
- Robo de un dispositivo móvil o de un archivo en papel que contenga Datos personales;
- Error humano (por ejemplo, un empleado envía accidentalmente un correo electrónico que contiene Datos personales a un destinatario no deseado, o altera o elimina accidentalmente Datos personales).
- Ataque cibernético (por ejemplo, abrir un archivo adjunto a un correo electrónico de un tercero desconocido que contenga software de rescate u otro software malicioso).
- Permitir el uso/acceso no autorizado (por ejemplo, permitir que un tercero no autorizado acceda a áreas seguras de las oficinas o sistemas de Entrust).
- Destrucción física y pérdida (por ejemplo, incendio o inundación); o
- Un tercero obtiene información de Entrust mediante engaño (por ejemplo, ataques de phishing o smishing).

Puede haberse producido un incidente con Datos personales por lo siguiente:

- Inicio de sesión inusual o actividad excesiva del sistema con respecto a las cuentas de usuario activas;
- Actividad inusual de acceso remoto;

- La presencia de falsas redes inalámbricas (Wi-Fi) visibles o accesibles desde el entorno de trabajo de Entrust;
- Fallo de los equipos; o
- Registradores de teclas de hardware o software conectados o instalados en sistemas de Entrust.

Los colegas que tengan conocimiento o cualquier motivo para sospechar que se ha producido o está a punto de producirse un incidente relacionado con Datos personales deben ponerse inmediatamente en contacto con el Centro de Operaciones de Seguridad de Entrust en SOC@entrust.com.

8.4 Respuesta a incidentes relacionados con datos personales

En caso de un incidente real o inminente relacionado con los Datos personales, Entrust aplicará sus procedimientos de respuesta y gestión de incidentes mantenidos por Seguridad de la Información para minimizar el impacto del incidente y notificar a los reguladores, a los interesados y a otras partes según se requiera legal o contractualmente. Una respuesta suele implicar lo siguiente:

- Investigar la filtración para determinar la naturaleza, causa y alcance del daño o perjuicio que pueda resultar;
- Implementar las medidas necesarias para evitar que la filtración continúe o se repita, y limitar el daño a los interesados afectados;
- Evaluar si existe la obligación de notificar a otras partes (por ejemplo, a las autoridades nacionales de protección de datos, a los interesados afectados, a las partes contractuales) y realizar dichas notificaciones de manera oportuna; y
- Registrar la información sobre el incidente de Datos personales y las medidas adoptadas en respuesta, incluida la documentación de las decisiones de notificar o no a los reguladores o a las partes afectadas.

9. Transparencia

Entrust proporciona transparencia con respecto a su programa global de privacidad de datos a través de sólidas páginas de destino internas y externas.

9.1 Avisos de privacidad

Entrust notifica a los interesados el Procesamiento de sus Datos personales tanto en calidad de controlador como procesador de datos. Esta información está disponible a través de los diversos avisos de privacidad de Entrust para usuarios de la web, solicitantes de empleo y colegas, así como a través de los avisos de privacidad de sus productos individuales disponibles aquí. Tales avisos proporcionan información sobre lo siguiente:

- Los tipos de Datos personales que trata Entrust;
- Finalidad y fundamento jurídico del Procesamiento;
- Terceros utilizados para el Procesamiento, si corresponde;

- Lugar y duración del Procesamiento;
- Cualquier transferencia transfronteriza de Datos personales;
- Duración del Procesamiento;
- Derechos del sujeto de datos; y
- Detalles de cualquier proceso de toma de decisiones automatizado o de inteligencia artificial

9.2 Formación

Entrust ofrece a sus empleados capacitación anual obligatoria sobre las responsabilidades en materia de protección de datos. Esta capacitación de introducción a la privacidad de datos se imparte en el momento de la incorporación y, posteriormente, en forma anual. Además de la Capacitación de Introducción a la Privacidad de Datos para todos los colegas, Entrust exige la realización anual de la Capacitación Mejorada en Privacidad de Datos por parte de los colegas que manejan datos sensibles y de categoría especial, así como la Capacitación en Privacidad por Diseño por parte de los colegas que desempeñan un papel en el desarrollo y diseño de ofertas de productos y servicios de software. Entrust sigue desarrollando e impartiendo capacitación adicional sobre privacidad específica para cada función, según sea necesario.

9.3 Derechos del sujeto de datos

Cuando Entrust procesa Datos personales, los sujetos de datos tienen determinados derechos en virtud de las leyes de protección de datos. Aunque estos derechos varían según la jurisdicción, los sujetos de datos suelen tener derecho a:

- Solicitar información sobre los Datos personales que Entrust posee sobre ellos, incluida una copia de dicha información;
- Rectificar los Datos personales inexactos y completar los Datos personales incompletos;
- Oponerse a que Entrust procese sus Datos personales cuando la Empresa lo haga en busca de sus propios intereses legítimos. Entrust puede continuar procesando los Datos personales a pesar de una objeción si los intereses legítimos de la Empresa superan a los del sujeto de datos, o si Entrust necesita hacerlo por motivos legales.
- Solicitar a Entrust que destruya los Datos personales que obran en su poder en relación con el sujeto de datos. La Empresa puede rechazar esta solicitud si los Datos personales siguen siendo necesarios para los fines para los que se están procesando y si existe una base legítima para que Entrust continúe procesándolos.
- Pedir a Entrust que limite el Procesamiento de sus Datos personales al almacenamiento en determinadas circunstancias.

Entrust evaluará los derechos del sujeto de datos en virtud de la legislación de protección de datos caso por caso y seguirá el Procedimiento de solicitud de datos del sujeto de datos (DSR) para determinar cómo satisfacer una solicitud. En general, Entrust utilizará los derechos de un sujeto de datos según el GDPR de la UE como base para cumplir con las solicitudes y aplicará los derechos adicionales disponibles con arreglo a la legislación de privacidad de datos aplicable en la medida en

que sean más favorables para el sujeto de datos. Si un sujeto de datos ejerce estos derechos y Entrust ha revelado los Datos personales en cuestión a un tercero, la Empresa hará todo lo posible para garantizar que el tercero también cumpla con los deseos del sujeto de datos.

Los sujetos de datos que deseen solicitar información sobre los Datos personales que Entrust tiene sobre ellos pueden hacerlo enviando una solicitud del sujeto de datos (DSR). Si los colegas reciben una solicitud directamente (ya sea verbalmente o por escrito), ésta deberá remitirse inmediatamente a privacy@entrust.com.

9.4 Autoridades supervisoras

La información de contacto de las autoridades supervisoras de datos relevantes varía según la ubicación. Encontrará la lista de las autoridades del Consejo Europeo de Protección de Datos aquí. La Oficina del Comisionado de Información (ICO) del Reino Unido (UK) puede encontrarse aquí. Aquí encontrará la Oficina del Comisionado de Privacidad de Canadá.

9.5 Delegado de protección de datos

A menos que se indique lo contrario, el Responsable de Protección de Datos de Entrust es:

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

10. Cumplimiento

Se espera que todos los colegas y trabajadores eventuales cumplan con esta política. Además, todas las unidades de negocio deben asegurarse de que cuentan con las normas y procedimientos locales adecuados para cumplir con esta política y la legislación aplicable en materia de privacidad de datos en su jurisdicción. Las infracciones de esta política se tomarán en serio y pueden resultar en acciones disciplinarias, incluido el despido. Esta política puede actualizarse o modificarse en cualquier momento.

11. Excepciones

No hay excepciones a esta política.

12. Propiedad e historial de revisiones

Esta política es responsabilidad del Director de Privacidad y se revisará anualmente.