ENTRUST

POLÍTICA GLOBAL DE PROTECCIÓN DE DATOS PERSONALES

Versión de documento	1.2
Fecha	10-sept-2020

Índice

1. Introducción

Como empresa y empleador, es necesario que Entrust Corporation y sus subsidiarias y filiales (colectivamente, «Entrust» o la «Empresa») recopilen, almacenen y procesen datos personales sobre nuestros empleados, trabajadores eventuales, clientes, proveedores y otros terceros con los que nos interactuamos para proporcionar productos o servicios en nuestro nombre.

Con la introducción del Reglamento General Europeo de Protección de Datos («RGPD») el 25 de mayo de 2018 y otras leyes aplicables que rigen la protección de datos, estamos sujetos a requisitos más estrictos con respecto a la forma en que recopilamos, utilizamos y almacenamos los datos personales.

2. Propósito

El propósito de esta política es ayudarnos a todos a cumplir con nuestras obligaciones legales y permitir que las personas sobre las que tenemos datos personales tengan confianza en nosotros. Esta política se aplica a todos los empleados de Entrust, trabajadores eventuales y terceros que tratan datos en nombre de Entrust. A menos que se especifique lo contrario, esta política se aplica en todos los países en los que Entrust opera o realiza actividades comerciales.

3. Requisitos de la póliza

3.1 Definiciones

«Responsable del tratamiento» se refiere a la entidad que determina el propósito y los medios del tratamiento de datos personales.

«Encargado del tratamiento» se refiere a la entidad que trata datos personales en nombre del responsable.

«Leyes de protección de datos» se refiere a todas las leyes y reglamentos aplicables de protección de datos y privacidad de datos, incluidos, entre otros, el Reglamento General de Protección de Datos de la UE (GDPR), la Ley de Protección Personal y Documentos Electrónicos de Canadá (PIPEDA) y la Ley de Privacidad del Consumidor de California (CCPA).

«Interesado» se refiere a la persona u hogar identificada o identificable con quien se relacionan los datos personales.

«Usuario de los datos» es un término utilizado para describir a cualquier empleado, consultor, contratista independiente, becario, trabajador temporal o tercero que actúe en nombre de Entrust (incluidos los encargados del tratamiento) cuyo trabajo implique el tratamiento de datos personales para Entrust.

«Información personal» tendrá el significado atribuido a «información de identificación personal», «información personal», «datos personales» o términos equivalentes según se definen en las leyes de protección de datos.

«Filtración de datos personales» tendrá el significado asignado por las leyes de protección de datos a los términos «filtración de seguridad», «violación de seguridad» o «violación de datos personales» e incluirá cualquier situación en la que el proveedor tenga conocimiento de que se ha accedido o es probable que se haya accedido a datos personales, y se hayan divulgado, alterado, perdido, destruido o utilizado por parte de personas no autorizadas, de manera no autorizada.

«Tratamiento» 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 tratamiento también incluye la transferencia o divulgación de datos personales a terceros.

«Datos de categoría especial» es un subconjunto de datos personales y se refiere a información sobre la raza u origen étnico, la vida sexual o la orientación sexual, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, los datos genéticos, los datos biométricos (color de ojos, color de pelo, estatura, peso), el historial médico o las condenas y delitos penales o las medidas de seguridad relacionadas de una persona.

3.2 Nuestra responsabilidad

Dependiendo de las circunstancias, Entrust puede actuar como controlador o responsable del tratamiento de datos. Como responsable del tratamiento, Entrust es responsable de establecer prácticas y políticas en consonancia con las leyes de protección de datos. Es igualmente importante que Entrust pueda demostrar el cumplimiento de estas leyes. La Empresa hace esto por medio de la:

- Implementación de políticas que permitan a la Empresa cumplir con las leyes de protección de datos, como esta política, las políticas sobre conservación de documentos y seguridad de datos, y las declaraciones de privacidad de Entrust.
- Comunicación y formación de los empleados, trabajadores eventuales y terceros que actúen en nombre de Entrust sobre los requisitos de protección de datos.
- Investigación de los casos de incumplimiento de las políticas de protección de datos de Entrust y toma de medidas correctivas o disciplinarias apropiadas.
- Investigación, remedios y, en algunos casos, notificar una filtración de datos personales.
- Realización de evaluaciones de impacto del tratamiento de datos cuando sea necesario para nuevos tipos de actividades de tratamiento.
- Realización de auditorías internas periódicas de las políticas y procedimientos de protección de datos de Entrust.
- Estudio de la protección de datos al inicio del diseño de nuevos productos.

3.3 Tratamiento de datos personales

Cualquier dato personal que la Empresa procese o que se procese en nombre de Entrust deberá:

- Ser tratado de manera justa, legal y transparente.
- Ser tratado únicamente para fines determinados, explícitos y legítimos.
- Ser pertinente y limitarse a lo necesario para los fines legítimos para los que se tratan los datos.
- Ser exactos y mantenerse actualizados asegurando, cuando sea razonablemente posible, que los datos personales inexactos sean borrados o rectificados sin demora.
- No conservarlo más tiempo del necesario para cumplir con el propósito o propósitos para los cuales se recopilaron.
- Ser tratado de manera que se garantice la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito, la pérdida accidental, la destrucción o el daño.

3.4 Bases jurídicas legales para el tratamiento de datos personales

La Empresa solo puede tratar datos personales si lo permiten las leyes de protección de datos. Los siguientes son los fundamentos en los que se basa Entrust para tratar los datos personales:

Cuando el tratamiento sea necesario:

- Para la ejecución de un contrato en el que el interesado sea parte, o para tomar medidas a petición del interesado antes de celebrar un contrato.
- Para el cumplimiento de una obligación legal a la que Entrust está sujeta.
- Para perseguir los intereses legítimos de Entrust, excepto cuando dichos intereses prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado.

Además de estos fundamentos, Entrust también podrá tratar datos personales cuando el interesado haya dado su consentimiento al tratamiento para uno o más fines específicos, siempre que el consentimiento sea libre, específico, informado y sea una indicación inequívoca de la voluntad del interesado. Cuando Entrust utiliza el consentimiento como fundamento para el tratamiento, el interesado tiene derecho a revocarlo en cualquier momento y por cualquier motivo.

En ocasiones, Entrust también puede necesitar tratar categorías especiales de datos personales para empleados o trabajadores eventuales (por ejemplo, cuando lo requieran las prácticas de empleo seguras). Cuando Entrust trata o utiliza a un tercero para tratar en su nombre categorías especiales de datos personales, Entrust se asegurará, en su caso, de que se cumplan las siguientes condiciones:

- El interesado ha dado su consentimiento explícito al tratamiento de la categoría especial de datos personales para uno o más fines específicos.

- El tratamiento es necesario para cumplir con las obligaciones derivadas de la legislación laboral, de la seguridad social o de la protección social, o de un convenio colectivo.
- El tratamiento es necesario para fines de medicina preventiva o laboral, o para la evaluación de la capacidad de trabajo de un empleado.
- El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona cuando esta se encuentre física o jurídicamente incapacitada para dar su consentimiento.
- El tratamiento se refiere a datos personales que han sido hechos públicos por el interesado y/o
- El tratamiento es necesario para establecer o defender reclamaciones legales.

3.5 Gestión de registros de datos

Entrust mantiene un registro central de los tipos de datos personales que la empresa recopila y la razón por la que se recopilan esos datos. Entrust solo tratará datos personales para el fin o fines específicos establecidos en el registro central o para cualquier otro fin específicamente permitido por las leyes de protección de datos. Entrust notificará a los interesados de esos fines cuando se recojan por primera vez o, cuando no sea posible, tan pronto como sea posible después.

Entrust solo tratará los datos personales en la medida en que sea necesario para los fines previstos para el interesado. Esto significa que Entrust no puede pedir ni registrar en sus sistemas más datos personales de los necesarios. La Empresa cuenta con las medidas técnicas y organizativas adecuadas para garantizar que los datos personales que ya no son necesarios sean borrados o destruidos.

La Empresa también emplea medidas razonables para asegurar que cualquier dato personal que se tenga sea exacto y se mantenga actualizado. El objetivo de Entrust es comprobar la exactitud de los datos personales en el momento de su recogida y, posteriormente, a intervalos regulares. La Empresa tomará todas las medidas razonables para borrar, destruir o modificar los datos inexactos o desactualizados sin demoras indebidas y, en cualquier caso, en el plazo de un mes a partir de la solicitud del interesado (o hasta tres meses cuando existan razones específicas por las que un mes no sea posible).

3.6 Borrado o destrucción de datos personales

Los registros en papel que contienen datos personales deben triturarse y eliminarse de forma segura cuando ya no sea necesario conservarlos. *Los registros en papel que contengan datos personales no podrán eliminarse de ninguna otra manera.*

Cuando se eliminen los datos personales electrónicos, deberán tomarse todas las medidas posibles para que los datos en cuestión sean inutilizables. Cuando sea imposible eliminar los datos personales por completo, se tomarán medidas razonables para garantizar que se eliminen en la mayor medida posible.

El departamento de informática es responsable de destruir o borrar los equipos electrónicos que contengan datos personales [por ejemplo, ordenadores portátiles, ordenadores de sobremesa, dispositivos móviles propiedad de la empresa y datos de trabajo en dispositivos «BYOD» (siglas en inglés de traiga su propio dispositivo)].

3.7 Seguridad de la información

Cuando la Empresa trata datos personales, toma medidas razonables para garantizar que los datos permanezcan seguros y estén protegidos contra el tratamiento no autorizado o ilegal, la pérdida accidental, la destrucción o el daño. Entrust hace esto por medio de:

- El cifrado de los datos personales siempre que sea posible y apropiado.
- La garantía de la confidencialidad, integridad, disponibilidad y resistencia permanentes de los sistemas y servicios utilizados para el tratamiento de los datos personales.
- La garantía del restablecimiento del acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico.
- La facilitación de la comprobación, valoración y evaluación de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los datos.

Al evaluar el nivel de seguridad adecuado, Entrust tiene en cuenta los riesgos asociados con el tratamiento, en particular los riesgos de destrucción accidental o ilícita, pérdida, alteración, divulgación no autorizada de los datos personales tratados o acceso a los mismos.

Cuando Entrust contrata a terceros para que procesen datos personales en su nombre, dichos terceros lo hacen sobre la base de instrucciones escritas, están sujetos a un deber de confidencialidad y están obligados a aplicar las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos. Los datos personales no se podrán compartir con ninguna persona ajena a Entrust o a terceros autorizados.

Los escritorios y armarios deben mantenerse cerrados con llave si contienen datos personales o información confidencial de cualquier tipo. Los usuarios de los datos deben asegurarse de que los monitores/pantallas individuales no muestren datos personales o información confidencial a quienes pasen por delante y de que cierren la sesión o bloqueen sus ordenadores/tabletas cuando los dejen desatendidos.

3.8 Información de una filtración de datos personales

Puede ocurrir una filtración de datos personales de muchas maneras, entre las que se incluyen:

- 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 impreso que contenga datos personales (por ejemplo, robo de un dispositivo en un vehículo o en el domicilio).
- 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).
- Circunstancias imprevistas como un incendio o una inundación.
- Cuando un tercero obtiene información de Entrust mediante engaño.

Entre los indicios de que puede haberse producido una filtración de los datos personales se incluyen los siguientes:

- Inicio de sesión inusual o actividad excesiva del sistema, en particular 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.
- Registradores de teclas de hardware o software conectados o instalados en sistemas Entrust.

Los compañeros que tengan conocimiento de alguna razón o tengan una razón para sospechar que se ha producido o está a punto de producirse una filtración de datos personales, póngase en contacto inmediatamente con el Centro de Operaciones de Seguridad de Entrust por correo electrónico en SOC@entrust.com y con la directora de cumplimiento en privacy@entrust.com.

3.9 Plan de respuesta a filtraciones de datos personales

En el caso de una filtración real o inminente de datos personales, Entrust tomará medidas rápidas para minimizar el impacto de la filtración e informará de ella si así lo requiere la ley. En la mayoría de los casos, la respuesta será:

- 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) y realizar dichas notificaciones. Si existe la obligación de notificar a las autoridades de protección de datos, la notificación debe realizarse normalmente en un plazo de 72 horas a partir del momento en que la empresa, incluido cualquiera de sus empleados, tenga conocimiento de la filtración.
- Registrar información sobre la filtración de los datos personales y las medidas adoptadas en respuesta, incluida la documentación que explique la decisión de notificar o no notificar.

3.10 Transferencias internacionales de datos y transferencias a terceros

Con arreglo al RGPD, Entrust puede transferir datos personales a países no pertenecientes al Espacio Económico Europeo («EEE») cuando exista un nivel adecuado de protección en ese país o cuando Entrust haya adoptado las medidas adecuadas para garantizar la protección de los datos.

Las empresas del grupo Entrust (por ejemplo, todas las entidades corporativas y subsidiarias) deben suscribir el Acuerdo de transferencia de datos dentro del grupo para garantizar las salvaguardias adecuadas para la transferencia de datos personales fuera del EEE, pero dentro del grupo Entrust.

Las empresas ajenas al grupo Entrust que tratan datos personales para o en nombre de Entrust, para las que Entrust actúa como controlador o responsable del tratamiento de datos, deben celebrar un acuerdo de tratamiento de datos con Entrust para garantizar las salvaguardias adecuadas para la transferencia de datos personales fuera del EEE. Dicho acuerdo contiene un lenguaje que garantiza que el tercero dispone de las medidas técnicas y organizativas adecuadas para cumplir con el RGPD y para garantizar la protección de los derechos de los interesados.

Los casos en los que Entrust transfiere datos personales a un país fuera del EEE pueden incluir:

- El interesado ha dado su consentimiento explícito a la transferencia propuesta después de que Entrust le haya informado de cualquier posible riesgo asociado con dicha transferencia (por ejemplo, la ausencia en ese país de salvaguardias equivalentes).
- La transferencia es necesaria para la ejecución de un contrato en el que el interesado sea parte, o para tomar medidas a petición del interesado antes de celebrar un contrato.
- La transferencia es necesaria para proteger los intereses vitales del interesado o de otra persona cuando este se encuentre física o jurídicamente incapacitado para dar su consentimiento.
- La transferencia es necesaria para el establecimiento o la defensa de una demanda judicial.

Por cada transferencia de datos fuera del EEE, Entrust se basará en las cláusulas contractuales estándar definidas por la Comisión Europea (2001/497/EC, 2004/915/EC y 2010/87/EU). Tenga en cuenta que también se requiere un acuerdo de transferencia de datos si se transfieren datos personales fuera de Canadá.

3.11 Notificación a los interesados

Entrust está obligada a proporcionar información a los interesados sobre el tratamiento de sus datos personales. Esta información se encuentra en la Declaración de privacidad de la empresa, disponible públicamente en www.entrust.com, y en la Declaración de privacidad de los empleados, disponible en la intranet de Entrust. Tales declaraciones proporcionan información sobre:

- Los tipos de datos personales que trata Entrust.
- El propósito y el fundamento jurídico del tratamiento de los datos personales.
- Si los datos personales serán revelados a terceros en el curso del tratamiento.
- Si los datos personales se transferirán fuera del EEE y Canadá y, en caso afirmativo, qué garantías se establecerán.
- Cuánto tiempo se tratarán los datos personales o, si no es posible determinarlo, los criterios que la Empresa utilizará para determinar el periodo de tratamiento.
- La forma en la que el interesado puede obtener una copia de sus datos personales en poder de Entrust.
- Los derechos del interesado, incluida la forma de presentar una reclamación.
- Si los datos personales deben tratarse para cumplir con una ley o un contrato, las posibles consecuencias de que el interesado no los facilite o se oponga al tratamiento.
- La existencia y los detalles de los procesos automatizados de toma de decisiones, en su caso.

Si Entrust recibe datos personales sobre un interesado de un tercero, la Empresa también proporcionará al interesado información sobre:

- el tipo de datos personales recibidos del tercero; y
- la fuente de los datos y si provienen de una fuente de acceso público (por ejemplo, un sitio web accesible al público).

3.12 Privacidad por diseño y evaluaciones de impacto de protección de datos

Las leyes de protección de datos requieren que Entrust considere la protección de datos durante las etapas de desarrollo de una nueva oferta de productos. Para cumplir con esta obligación, Entrust debe tomar medidas para asegurar que la protección de datos forme parte del proceso de diseño y que la recopilación de datos personales se reduzca al mínimo en la medida de lo posible.

En algunas circunstancias (a saber, cuando el tratamiento suponga un riesgo elevado para los derechos y libertades de la persona), puede exigirse a Entrust que lleve a cabo una evaluación formal del impacto de la protección de datos en relación con el tratamiento de datos personales. Dicha evaluación incluye la documentación de los fines para los que se lleva a cabo la actividad, la forma en la que Entrust cumplirá con las leyes de protección de datos y cómo la empresa reducirá los riesgos potenciales para la privacidad de las personas. Si cree que puede ser necesaria una evaluación del impacto de la protección de datos, póngase en contacto con la directora de cumplimiento en privacy@entrust.com.

3.13 Derechos del interesado

Si Entrust procesa datos personales, según las leyes de protección de datos, el interesado puede tener derecho a:

- Solicitar información sobre los datos personales que obran en su poder.
- Hacer que se rellenen y corrijan todos los datos personales inexactos sobre ellos, sin perjuicio de que Entrust determine que los datos son, de hecho, inexactos o incompletos.
- Oponerse a que Entrust procese sus datos personales cuando la Empresa lo haga en busca de sus propios intereses legítimos. Entrust puede continuar tratando los datos personales a pesar de una objeción si los intereses legítimos de la Empresa superan a los del interesado, o si Entrust necesita hacerlo para establecer o defender una demanda judicial.
- Solicitar a Entrust que destruya los datos personales que obran en su poder en relación con el interesado. La Empresa puede rechazar esta solicitud si los datos personales siguen siendo necesarios para los fines para los que se están tratando y si existe una base legítima para que Entrust continúe procesándolos.
- Solicitar a Entrust que limite el tratamiento de sus datos personales al almacenamiento. Esto solo puede solicitarse si la exactitud de los datos personales ha sido impugnada y permanece sin verificar; Entrust ya no requiere los datos personales, pero el interesado los necesita para establecer o defender una demanda judicial; el interesado se ha opuesto al tratamiento de datos personales; y Entrust está decidiendo si sus intereses legítimos prevalecen sobre los intereses del interesado o si el tratamiento es ilegal.

Si un interesado 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 interesado.

3.14 Solicitudes de acceso del interesado

Los interesados que deseen solicitar información sobre los datos personales que Entrust tiene sobre ellos pueden hacerlo enviando una Solicitud de acceso al interesado (DSAR, por sus siglas en inglés). Si los compañeros reciben una solicitud directamente (ya sea verbalmente o por escrito), envíe inmediatamente los detalles de la solicitud a privacy@entrust.com.

3.15 Formación

Entrust proporciona a sus empleados y trabajadores eventuales acceso a formación sobre las responsabilidades de protección de datos. Esta formación se imparte al incorporarse a la empresa y a intervalos regulares a partir de entonces.

3.16 Directora general de protección de datos

La representante asignada para el RGPD de Entrust es Anjali Doherty, abogada corporativa superior (Reino Unido). El director de protección de datos de Entrust Deutschland GmbH es el bufete de abogados de Kill & Wolff GmbH. Entrust Corporation no tiene un director de protección asignado. La supervisión del programa de cumplimiento de privacidad de datos está a cargo de la directora de cumplimiento, Jenny Carmichael, que se encuentra en las oficinas centrales de Entrust en Shakopee, Minnesota (Estados Unidos).

4. Cumplimiento

Se espera que todos los empleados 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 ser actualizada o enmendada en cualquier momento.

5. Excepciones

No hay excepciones a esta política.

6. Propiedad y revisión

Esta política es propiedad de la consejera general/directora de cumplimiento. Esta política se revisará anualmente. Los cambios a este documento se harán de conformidad con la Norma de control de documentos y registros del ISMS.

6.1 Información de contacto

Las preguntas sobre esta política o las quejas sobre el manejo de los datos personales deben dirigirse a la directora de cumplimiento en privacy@entrust.com.