Salvaguardas de Accenture
en relación con los datos de sus clientes

Los siguientes términos describen las medidas técnicas y organizativas, los controles internos y las rutinas de seguridad de la información que Accenture mantiene para salvaguardar los datos proporcionados por o en nombre de nuestros clientes en relación con un compromiso de servicio al cliente ("Datos de cliente"). Estas medidas de seguridad pretenden proteger los Datos de cliente cuando se encuentran en los entornos de Accenture (por ejemplo, sistemas, redes, instalaciones) contra su acceso accidental, no autorizado o ilegal, su divulgación, alteración, pérdida o su destrucción. Cuando los Datos de cliente incluyan datos personales, la implementación y el cumplimiento de estas medidas (y cualquier otra medida de seguridad adicional establecida en el contrato con el cliente que resulte de aplicación) están diseñados para proporcionar un nivel adecuado de seguridad con respecto al procesamiento de los datos personales. Accenture puede modificar estas medidas, sin previo aviso, siempre y cuando dichas revisiones no reduzcan o degraden materialmente la protección de los Datos de cliente.

SALVAGUARDAS ESTÁNDAR EN RELACIÓN CON LOS DATOS DEL CLIENTE:

1. Organización de la seguridad de la información

a. Propiedad de la seguridad. Accenture nombrará a uno o varios responsables de seguridad encargados de coordinar y supervisar las normas y procedimientos de seguridad.

b. Funciones y responsabilidades de seguridad. El personal de Accenture con acceso a los Datos de cliente estará sujeto a obligaciones de confidencialidad.

c. Programa de gestión de riesgos. Accenture contará con un programa de gestión de riesgos para identificar, evaluar y tomar las medidas adecuadas con respecto a los riesgos relacionados con el procesamiento de los Datos de cliente en relación con el contrato formalizado con el cliente.

2. Gestión de activos

a. Inventario de activos. Accenture mantendrá un inventario de activos de su infraestructura, red, aplicaciones y entornos en la nube. Accenture también mantendrá un inventario de sus soportes en los que se almacenan los Datos de cliente. El acceso a los inventarios de dichos medios estará restringido al personal autorizado por escrito para tener dicho acceso.

b. Manejo de datos. Accenture

i. Clasificará los Datos de cliente para ayudar a identificarlos y permitir que el acceso a los mismos se restrinja adecuadamente.

ii. Limitará la impresión de Datos de cliente desde sus sistemas a lo mínimamente necesario para realizar los servicios y tendrá procedimientos para eliminar los materiales impresos que contengan Datos de cliente.

iii. Exigirá a su personal que obtenga la autorización adecuada antes de almacenar los Datos de cliente fuera de los lugares y sistemas aprobados contractualmente, acceder de forma remota a los Datos de cliente o procesar los Datos de cliente fuera de las instalaciones de las Partes.

3. **Seguridad de los recursos humanos**

   a. **Formación en materia de seguridad**. Accenture

      i. Informará a su personal sobre los procedimientos de seguridad pertinentes y sus respectivas funciones.

      ii. Informará a su personal de las posibles consecuencias de infringir las normas y procedimientos de seguridad.

      iii. Utilizará únicamente datos anónimos en sus entornos de formación.

4. **Seguridad física y medioambiental**

   a. **Acceso físico a las instalaciones**. Accenture implantará y mantendrá procedimientos para limitar el acceso a sus instalaciones donde se encuentran los sistemas de información que procesan los Datos de cliente.

   b. **Acceso físico a los componentes**. Accenture mantendrá registros de los soportes entrantes y salientes que contengan Datos de cliente, incluyendo el tipo de soporte, los remitentes/receptores autorizados, la fecha y la hora, el número de soportes y los tipos de Datos de cliente que contienen.

   c. **Eliminación de componentes**. Accenture utilizará los procesos estándar del sector (por ejemplo, ISO 27001, CIS Sans 20 y/o NIST Cyber-Security Framework, según corresponda) para eliminar los Datos de cliente cuando ya no sean necesarios.

5. **Gestión de comunicaciones y operaciones**

   a. **Política operativa**. Accenture mantendrá documentos de seguridad que describan sus medidas de seguridad y los procedimientos y responsabilidades pertinentes de su personal que tenga acceso a los Datos de cliente.

   b. **Gestión de Dispositivos Móviles (MDM) /Gestión de Aplicaciones Móviles (MAM)**. Accenture mantendrá una política para sus dispositivos móviles que:

      i. Imponga la encriptación de los dispositivos.

      ii. Prohíba el uso de aplicaciones de la lista negra.

      iii. Prohíba la inscripción de dispositivos móviles que hayan sido "jail broken".

   c. **Procedimientos de recuperación de datos**. Accenture deberá

      i. Tener procedimientos específicos de recuperación de datos relacionados con sus sistemas, diseñados para permitir la recuperación de los Datos de cliente que se mantienen en sus sistemas.

      ii. Revisar sus procedimientos de recuperación de datos al menos una vez al año.

      iii. Registrar la actividad de restauración de datos con respecto a sus sistemas, incluyendo la persona responsable, la descripción de los datos restaurados y, en su caso, la persona responsable y qué datos (si los hay) tuvieron que ser introducidos manualmente en el proceso de recuperación de datos.

   d. **Software malicioso**. Accenture tendrá controles antimalware para ayudar a evitar que el software malicioso obtenga acceso no autorizado a los Datos de cliente, incluido el software malicioso que se origina en las redes públicas.

e. Datos fuera de sus instalaciones. Accenture

i. Cifrará los datos de los clientes que se transmitan a través de redes públicas.

ii. Protegerá los Datos de cliente en los medios que salgan de sus instalaciones (por ejemplo, mediante el cifrado).

iii. Implementará herramientas automatizadas, siempre que sea posible, para reducir los riesgos de los correos electrónicos, cartas y/o faxes mal dirigidos desde sus sistemas.

f. Registro de eventos.

i. En los sistemas de Accenture que contengan Datos de cliente, Accenture registrará los eventos de acuerdo con sus políticas o normas internas.

6. Control de acceso

a. Política de acceso. Accenture mantendrá un registro de los privilegios de seguridad de las personas que tienen acceso a los Datos de cliente a través de sus sistemas.

b. Autorización de acceso. Accenture deberá

i. Mantener y actualizar un registro del personal autorizado a acceder a los Datos de cliente a través de sus sistemas.

ii. Cuando sea responsable de la provisión de acceso, proporcionará rápidamente las credenciales de autenticación.

iii. Desactivar las credenciales de autenticación cuando no se hayan utilizado durante un período de tiempo (dicho período de no utilización no debe superar los 90 días).

iv. Desactivar las credenciales de autenticación cuando se notifique que el acceso ya no es necesario (por ejemplo, por el cese de un empleado, la reasignación de un proyecto, etc.) en un plazo de 2 días hábiles.

v. Identificar al personal que puede conceder, modificar o cancelar el acceso autorizado a los datos y recursos.

vi. Garantizar que, cuando más de un individuo tenga acceso a sus sistemas que contienen Datos de cliente, los individuos tengan identificadores/contactos únicos (es decir, que no se compartan identificadores).

c. Mínimo privilegio. Accenture

i. Sólo permitirá que su personal de soporte técnico tenga acceso a los Datos de cliente cuando sea necesario.

ii. Mantendrá controles que permitan el acceso de emergencia a los sistemas de producción a través de identificadores firefighter, identificadores temporales o identificadores gestionados por una solución de Gestión de Acceso Privilegiado.

iii. Restringirá el acceso a los Datos de cliente en sus sistemas sólo a aquellas personas que requieran dicho acceso para realizar su función laboral.

iv. Limitará el acceso a los Datos de cliente en sus sistemas sólo a los datos mínimamente necesarios para realizar los servicios.

v. Apoyará la segregación de funciones entre sus entornos para que ninguna persona tenga acceso a realizar tareas que creen un conflicto de intereses en materia de seguridad (por ejemplo, desarrollador/revisor, desarrollador/probador).

d. Integridad y confidencialidad. Accenture instruirá a su personal para que desactive las sesiones administrativas cuando abandone las instalaciones o cuando los ordenadores queden desatendidos.

e. Autenticación. Accenture

i. Utilizará las prácticas estándar del sector (por ejemplo, ISO 27001, CIS Sans 20, y/o NIST Cyber-Security Framework, según corresponda) para identificar y autenticar a los usuarios que intenten acceder a sus sistemas de información.

ii. Cuando los mecanismos de autenticación se basen en contraseñas, exigirá que las contraseñas se renueven periódicamente.

iii. Cuando los mecanismos de autenticación se basen en contraseñas, exigirá que la contraseña contenga al menos 8 caracteres y 3 de los siguientes 4 tipos de caracteres: numéricos (0-9), minúscula (a-z), mayúscula (A-Z), especiales (por ejemplo, !, *, &, etc.).

iv. Se asegurará de que los identificadores desactivados o caducados no se conceden a otras personas.

v. Controlará los intentos repetidos de acceder a sus sistemas de información utilizando una contraseña no válida.

vi. Mantendrá los procedimientos estándar de la industria (por ejemplo, ISO 27001, CIS Sans 20 y/o el Marco de Ciberseguridad del NIST, según corresponda) para desactivar las contraseñas que hayan sido corrompidas o reveladas inadvertidamente.

vii. Utilizará prácticas de protección de contraseñas estándar del sector (por ejemplo, ISO 27001, CIS Sans 20 y/o NIST Cyber-Security Framework, según corresponda), incluyendo prácticas diseñadas para mantener la confidencialidad e integridad de las contraseñas cuando se asignan y distribuyen, así como durante su almacenamiento.

f. Autenticación de múltiples factores. Accenture implementará la Autenticación de Factores Múltiples para el acceso interno y el acceso remoto a través de la red privada virtual (VPN) a sus sistemas.

7. Pruebas de penetración y análisis de vulnerabilidad de los sistemas de Accenture.

a. Al menos una vez al año, Accenture realizará evaluaciones de penetración y vulnerabilidad en los entornos informáticos de Accenture de acuerdo con las políticas de seguridad internas y las prácticas estándar de Accenture.

b. Accenture se compromete a compartir con el cliente la información resumida relacionada con dichas pruebas realizadas por Accenture en la medida en que sea aplicable a los Servicios.

c. Para mayor claridad, en lo que respecta a dichas pruebas de penetración y vulnerabilidad, el cliente no tendrá derecho a (i) recibir datos o información de otros clientes de Accenture; (ii) probar entornos de TI de terceros, excepto en la medida en que Accenture tenga derecho a permitir dichas pruebas; (iii) cualquier acceso o prueba de infraestructura o entornos de servicios compartidos, o (iv) cualquier otra información confidencial de Accenture que no sea directamente relevante para dichas pruebas y los Servicios.

d. En el caso de los sistemas informáticos de Accenture que estén físicamente dedicados al cliente, las Partes podrán acordar planes de prueba separados y por escrito, y dichas pruebas no excederán de 2 pruebas al año.

8. **Diseño y gestión de redes y aplicaciones**. Accenture deberá

   a. Tener controles para evitar que las personas obtengan acceso no autorizado a los Datos de cliente en sus sistemas.

   b. Utilizar procedimientos de prevención de pérdida de datos basados en correo electrónico para supervisar o prevenir movimientos de datos sensibles.

   c. Utilizar el filtrado web basado en la red para evitar el acceso a sitios no autorizados.

   d. Utilizar identificaciones firefighter o de usuarios temporales para el acceso a la producción.

   e. Utilizar la detección y/o prevención de intrusiones en la red en sus sistemas.

   f. Utilizar estándares de codificación seguros.

   g. Buscar y reparar las vulnerabilidades de OWASP en sus sistemas.

   h. En la medida que sea técnicamente posible, se espera que las Partes trabajen juntas para limitar la capacidad del personal de Accenture para acceder a entornos que no son del cliente ni de Accenture desde los sistemas del cliente.

   i. Mantenwe actualizados los estándares de configuración de seguridad de servidor, red, infraestructura, aplicaciones y nube.

   j. Escanear sus entornos para asegurarse de que se hayan solucionado las vulnerabilidades de configuración identificadas.

9. **Gestión de parches**

   a. Accenture tendrá un procedimiento de administración de parches que implemente parches de seguridad para sus sistemas utilizados para procesar Datos de cliente que incluye:

      i. Tiempo definido permitido para implementar parches (que no exceda los 90 días para parches altos o medianos según lo definido por el estándar de Accenture); y

      ii. Proceso establecido para manejar parches críticos o de emergencia tan pronto como sea posible.

10. **Estaciones de trabajo**

   a. Accenture implementará controles para las estaciones de trabajo que proporcione en relación con la prestación de servicios que incorporan lo siguiente:

      i. Software agente que gestiona el cumplimiento general de la estación de trabajo e informa como mínimo semanalmente a un servidor central.

      ii. Disco duro encriptado.

      iii. Proceso de parcheo para que las estaciones de trabajo estén parcheadas dentro del programa de parcheo documentado.

      iv. Capacidad para evitar que se instale software incluido en la lista negra.

      v. Antivirus con un escaneo mínimo semanal.

      vi. Cortafuegos instalados.

11. Gestión de infracciones de seguridad de la información

a. Proceso de respuesta a violaciones de seguridad. Accenture mantendrá un registro de sus propias infracciones de seguridad en sus sistemas con una descripción de la infracción, el período de tiempo, las consecuencias de la infracción, el nombre del denunciante, a quién se informó la infracción y el proceso de recuperación de datos.

b. Monitoreo de servicios. El personal de seguridad de Accenture revisará sus propios registros como parte de su proceso de respuesta a brechas de seguridad para proponer esfuerzos de remediación si es necesario.

12. Gestión de la continuidad del negocio

a. Accenture tendrá procesos y programas que están alineados con ISO 22301 para permitir la recuperación de sucesos que impactan en su capacidad para ejecutar servicios según lo establecido en contractualmente con su cliente.

MEDIDAS COMPLEMENTARIAS: Adicionalmente, de conformidad con las directrices regulatorias derivadas de la decisión "Schrems II" del Tribunal de Justicia de la Unión Europea, Accenture se compromete a mantener las siguientes medidas técnicas, organizativas y legales/contractuales adicionales con respecto a los Datos de cliente, incluidos los datos personales.

Medidas Técnicas Complementarias:

1. Los Datos de cliente en tránsito entre las entidades de Accenture estarán fuertemente encriptados con un cifrado que:

a. es de última generación,

b. asegura la confidencialidad por el período de tiempo requerido,

c. se implementa mediante un software debidamente mantenido,

d. es robusto y otorga protección contra ataques activos y pasivos por parte de las autoridades, incluido el análisis criptográfico, y

e. no contiene puertas traseras en hardware o software, a menos que se acuerde lo contrario con un cliente concreto.

2. Los Datos de cliente en reposo y almacenados por cualquier entidad de Accenture estarán fuertemente encriptados con un cifrado que:

a. es de última generación,

b. asegura la confidencialidad por el período de tiempo requerido,

c. se implementa mediante un software debidamente mantenido,

d. es robusto y otorga protección contra ataques activos y pasivos por parte de las autoridades, incluido el análisis criptográfico, y

e. no contiene puertas traseras en hardware o software, a menos que se acuerde lo contrario con un cliente concreto.

Medidas complementarias organizativas:

1. La transferencia de Datos de cliente entre entidades de Accenture y el procesamiento por cualquiera de las entidades de Accenture se realizará de conformidad con:

a. las políticas y procedimientos internos de Accenture para gestionar las solicitudes de acceso a datos personales de las autoridades,

b. las políticas y procedimientos de confidencialidad y acceso a datos internos de Accenture,

c. las políticas y procedimientos internos de minimización de datos de Accenture, y

d. las políticas y procedimientos internos de seguridad y privacidad de datos de Accenture.

2. Accenture mantendrá un registro documentado de las solicitudes de acceso a datos personales recibidas de las autoridades y de la respuesta dada, junto con la justificación legal y las partes involucradas.

3. Accenture proporcionará regularmente informes de solicitudes de datos personales de las autoridades, si las hubiera, al Chief Compliance Officer de Accenture.

Medidas Complementarias Legales/Contractuales:

1. Accenture mantendrá informes de evaluación actualizados regularmente con respecto a las leyes de vigilancia y las prácticas de privacidad para aquellos países en los que Accenture procese Datos de cliente si dicho país no está formalmente reconocido como país que otorga un nivel de protección esencialmente similar al de los países de la UE y proporcionará copias de dichos informes a los clientes que lo soliciten.

2. Las entidades de Accenture que procesen los Datos de cliente certifican, a menos que se acuerde lo contrario con un cliente concreto, que (a) no han creado intencionalmente puertas traseras o programación similar que pueda usarse para acceder al sistema y/o a los datos personales (b) no han creado o cambiado intencionalmente sus procesos comerciales de forma que facilite el acceso a datos personales o sistemas, y (c) Accenture entiende que la ley nacional aplicable o la política gubernamental no requieren que las entidades de Accenture creen o mantengan puertas traseras o faciliten el acceso a datos personales o sistemas o posean o entreguen la clave de cifrado sin una orden legalmente válida y tras una revisión legal adecuada.

3. En la medida en que lo permita la ley aplicable, las entidades de Accenture que procesen los Datos de cliente informarán al cliente sobre las solicitudes gubernamentales relacionadas con los datos personales que Accenture esté procesando en nombre del cliente. Si, de conformidad a la ley aplicable, a Accenture no se le permite informar al cliente sobre una solicitud gubernamental, Accenture tomará las medidas razonables para (i) obtener la autorización administrativa o judicial para informar al cliente lo antes posible o (ii) solicitar que la autoridad gubernamental correspondiente informe directamente al cliente. En cualquier caso, Accenture tomará las medidas razonables ante los tribunales o en procedimientos administrativos para impugnar las solicitudes gubernamentales que considere ilegales.

4. Accenture informará al cliente que corresponda de cualquier cambio en la ley aplicable que pudiera afectar la capacidad de Accenture para cumplir con el mecanismo de transferencia de datos en el que se basa.

5. Las entidades de Accenture que procesen los Datos de cliente permitirán que el cliente correspondiente verifique si sus datos personales se divulgaron a las autoridades a través de procedimientos de auditoría acordados según lo establecido en el contrato formalizado con el cliente que corresponda.

6. Las entidades de Accenture que procesen los Datos de cliente no formarán parte de ninguna transferencia posterior de los Datos de cliente, ni suspenderán las transferencias en curso, sin la aprobación del cliente según se establezca en el contrato con el cliente que corresponda o según lo exija la ley.

7. Nada de lo aquí dispuesto impedirá al interesado ejercitar su derecho a reclamar daños a Accenture según lo permitido por la ley aplicable en caso de que Accenture

divulgue los Datos de cliente transferidos incumpliendo sus obligaciones incluidas en la herramienta de transferencia elegida.