Política de Seguridad

1. Preámbulo
El objeto, el alcance, la naturaleza y la finalidad del tratamiento de los datos se derivarán de la relación comercial cuya base es el contrato de venta y mantenimiento celebrado entre las partes y que sustituye a todos los acuerdos anteriores en esta materia. Las presentes Medidas de Seguridad complementarán el contrato de venta celebrado entre el Cliente y Axess en lo que respecta al tratamiento de los datos del cliente y se considerarán parte integrante del mismo. Axess garantizará las siguientes medidas de seguridad informática en el marco de la relación comercial entre Axess y el Cliente.

2. Medidas técnicas y organizativas generales
Axess siempre adoptará todas las medidas necesarias de conformidad con el RGPD para el tratamiento de los datos transferidos a los sistemas de procesamiento de datos. Garantiza que la organización interna está diseñada para cumplir con los requisitos relativos a la protección de datos. Las siguientes condiciones se aplicarán independientemente del lugar en el que esté alojado el servidor.

2.1 Control del uso previsto:
Las medidas que se indican a continuación garantizan que los datos recabados para fines diferentes serán objeto de tratamiento también por separado:
> Datos basados en software (por ejemplo, discriminación de clientes)
> Discriminación a través de la regulación del acceso (principio de la base de datos)
> Discriminación de los datos de prueba y de los datos actuales
> Discriminación de los sistemas de prueba y de los sistemas actuales (tecnología, programas)

2.2 Seudonimización
En la medida de lo posible, para cada tratamiento de datos se eliminarán las características primarias de identificación de los datos personales en la respectiva aplicación de datos y se almacenarán por separado.

2.3 Control de entrada:
Se garantiza que se podrá comprobar y decidir a posteriori si los datos personales se introducen, se modifican o se eliminan de los sistemas de tratamiento de datos y quién lo hace. A tal fin, Axess documentará o registrará las entradas/archivos de registro.

2.4 Privacidad desde el Diseño y Privacidad predeterminada
Unos ajustes predeterminados adecuados, como parte integrante de las medidas técnicas y organizativas, garantizan que, por principio, solo serán objeto de tratamiento aquellos datos personales cuyo tratamiento sea necesario para la finalidad especificada de dicho tratamiento.
> Solo se recabarán datos personales si son necesarios para la gestión del contrato de venta (por ejemplo abonos de temporada, etc.).
> La configuración de las cookies en las tiendas online de Axess sólo será posible con el consentimiento del usuario.
> El uso de los datos personales para fines de marketing sólo se permitirá con el consentimiento expreso del usuario.

3 Medidas técnicas y organizativas en caso de servidores alojados por Axess
Si el cliente utiliza el SERVICIO DE CENTRO DE DATOS de Axess, se garantiza que se definirán las áreas de seguridad y el círculo de personas autorizadas o las autorizaciones de acceso, que las vías de acceso estarán aseguradas adecuadamente y que los soportes de registro de datos estarán controlados y almacenados de forma segura. Las medidas que se indican a continuación sólo serán de aplicación si el servidor está alojado por Axess.

3.1 Control de admisión:
Las personas no autorizadas tendrán prohibido el acceso a los sistemas de tratamiento de datos a través de los cuales se tratan o utilizan dichos datos. Las salas de ordenadores están situadas en un edificio de oficinas clasificado como sismorresistente. Solamente los empleados de informática, los de las propias instalaciones y la dirección tendrán acceso a dichas instalaciones. El control de acceso se garantiza a través de las siguientes medidas:
> Autorización / Tarjeta chip

La presencia en la zona de seguridad quedará registrada. El personal no autorizado y personas ajenas a la empresa (técnicos de mantenimiento, asesores, personal de limpieza, etc.) sólo podrán acceder a las salas cuando sean acompañados por personas autorizadas. El control de admisión se realizará mediante las siguientes medidas técnico-organizativas adicionales:
> Sistema de alarma
> Vigilancia del edificio
> Videotecnología

3.2 Control de entrada:
El uso de los sistemas de tratamiento de datos por personas no autorizadas se impedirá a través de las siguientes medidas:
> Contraseña
Cada persona autorizada dispondrá de su propia contraseña, que solo ella conoce y que debe cambiarse periódicamente. Se crearán protocolos automáticos (archivos de registro) relativos a todas las actividades del sistema de procesamiento de datos y telecomunicaciones. El uso de los sistemas de procesamiento de datos con la ayuda de equipos para la transmisión de datos por parte de personas no autorizadas se impedirá a través de las siguientes medidas:
> VPN (Red Privada Virtual)

3.3 Control de acceso:
Se garantiza que las personas autorizadas a emplear un sistema de tratamiento de datos sólo podrán acceder a aquellos datos que requieran autorización de acceso y que sin dicha autorización, los datos no podrán ser leídos, copiados, modificados o eliminados durante el tratamiento, uso o almacenamiento. La restricción a la posibilidad de acceso de la persona autorizada exclusivamente a los datos sujetos a su autorización de acceso estará garantizada por las siguientes medidas:
> Comprobación automática de la autorización de acceso (en el sistema)

3.4 Control de transferencia:
Se garantiza que los datos personales no podrán ser leídos, copiados, modificados o eliminados sin autorización durante la transmisión electrónica o durante su transporte o almacenamiento en soportes de registro de datos, y que se podrá comprobar y determinar en qué momento se prevé una transferencia de datos personales mediante dispositivos de transferencia de datos. El envío de soportes de registro de datos se documentará y se controlará mediante su registro y la documentación adjuntada. No se permitirá traer ni utilizar soportes privados de registro de datos en las salas. Los soportes de registro de datos se destruirán de la siguiente manera:
> En el caso de soportes magnéticos de datos, mediante sobrescritura y destrucción física (por un proveedor de servicios externo)
En la medida en que se utilice Internet para reenviar datos personales, se emplearán las siguientes medidas de seguridad:
> Firewall
> Red Privada Virtual (VPN)

3.5 Control de disponibilidad:
Las siguientes medidas garantizan que los datos personales estarán protegidos contra su destrucción o pérdida accidental:
> Copia de seguridad diaria/semanal/mensual/anual de los datos
> Red de área de almacenamiento (SAN)
> Duplicación en espejo de los discos (entre otros, RAID)
> Sistema ininterrumpido de alimentación eléctrica (UPS)
> Protector de sobretensión
> Generador de emergencia
> Externalización de datos
> Dispositivos de prevención de incendios

3.6 Gestión de la protección de datos
Se garantiza que se ha creado e implementado un sistema de gestión de la protección de datos. La gestión de protección de datos se desglosa en los siguientes aspectos:
> Listado de las actividades de tratamiento de datos
> Tratamiento de datos contractuales
> Evaluación del impacto sobre la protección de datos
> Gestión de respuesta ante incidentes
> Informes sobre violaciones de la protección de datos
> Formación
> PHVA (Planificar, Hacer, Verificar y Actuar) (en inglés, PDCA): controles regulares

3.7 Gestión de la respuesta ante incidentes
Se han adoptado medidas sobre el modo en que las personas responsables deben reaccionar ante posibles escenarios. Éstos incluyen violaciones de la seguridad de los datos, DoS (denegación de servicio), DDoS (denegación distribuida de servicio), brechas en el firewall, presencia de virus o malware y amenazas por parte de agentes internos.
La gestión de respuesta ante incidentes se divide en seis fases importantes:
> Preparación: Tanto los usuarios como los empleados informáticos están formados o informados de que pueden ocurrir incidentes y de las medidas que deben adoptar ante ellos.
> Identificación: Toma de decisiones sobre si un supuesto supone un incidente de protección de datos.
> Confinamiento: Para limitar los daños causados por el incidente y aislar los sistemas afectados al objeto de evitar más daños.
> Erradicación: Para hallar la causa o el desencadenante del incidente y para retirar los sistemas afectados del entorno productivo.
> Recuperación: Para integrar de nuevo los sistemas afectados en el entorno productivo, una vez quede asegurado que no existen más amenazas.
> Conocimientos adquiridos: Finalización de la documentación relativa al incidente y análisis de todo aquello que el equipo o la empresa pueden aprender del incidente. De este modo se podrán mejorar las respuestas futuras ante ciertas circunstancias.

4 Acceso a Datos del Cliente
Con el fin de proporcionar el apoyo adecuado en caso de que surjan problemas, Axess, en tanto que gestor de datos, se reserva el derecho de acceder al sistema o datos del Cliente, siempre que dicho acceso esté amparado por el contrato de venta entre Axess y el Cliente, o el Cliente haya dado su consentimiento para dicho acceso, o el revendedor haya transmitido a Axess la solicitud de servicio requerida en nombre del Cliente.

Política de Seguridad

Axess garantiza que:
> Solo podrá haber acceso físico al hardware del centro de datos si el cliente adquiere el Servicio de Centro de Datos de Axess;
> El acceso a los datos del Cliente a través de la herramienta de mantenimiento remoto se producirá solo en el caso descrito anteriormente y con el consentimiento o en nombre del Revendedor y/o del Cliente.
> El acceso a los dispositivos locales solo se permitirá en caso de que el cliente o el revendedor soliciten ayuda.

5 Tratamiento de pedidos:
Como complemento a la presente relación comercial, las presentes disposiciones sobre tratamiento de datos por encargo garantizan que se cumplen todas las obligaciones mutuas con arreglo al Reglamento General sobre Protección de Datos. („RGPD“).

Axess procesará datos personales en nombre del Cliente, por lo que el tema, el alcance, el tipo, las categorías de datos procesados, el propósito del procesamiento, así como las categorías de interesados (Datos del Cliente) emanarán del respectivo contrato de venta celebrado entre las partes contractuales. Por lo tanto, las disposiciones sobre el tratamiento de datos por encargo complementarán todos los acuerdos celebrados entre el Cliente y Axess en la medida en que se relacionen con el tratamiento de datos personales.

El tratamiento de datos por parte de Axess se llevará a cabo exclusivamente en un Estado miembro de la Unión Europea, por lo que el tratamiento transfronterizo de datos, de conformidad con el Artículo 4 línea 23 del RGPD (dentro de la Unión), debe notificarse a su debido tiempo al Cliente, como parte responsable, antes del inicio del tratamiento, de tal modo que el Cliente pueda presentar objeciones. El silencio ante esta notificación implicará el consentimiento para dicho tratamiento.

5.1 Obligaciones del Gestor de datos:
Mediante la firma del contrato de compraventa, el cliente acepta las medidas técnicas y organizativas establecidas en esta política. Al implementar esta política y cumplir con las instrucciones generales e individuales del cliente con respecto a los datos personales (por ejemplo, sobre eliminación de datos del cliente, anonimización de datos), Axess garantiza un nivel de protección de última tecnología sobre las aplicaciones de los datos objeto del contrato, de modo que solo se podrán presentar reclamaciones de cualquier tipo en caso de incumplimiento.

Cualesquiera cambios en las medidas técnicas y organizativas que garanticen un nivel constante de protección de los datos personales procesados o aumenten dicho nivel se considerarán aprobados y se comunicarán al Cliente si éste lo solicita, pero Axess no tendrá obligación de ponerlos en conocimiento del Cliente.

Axess adoptará las medidas técnicas y organizativas descritas anteriormente para asegurar que el Cliente respeta los derechos de los interesados en virtud del Capítulo III del RGPD (información, acceso, rectificación, eliminación, restricción, portabilidad de datos, objeción y toma de decisiones automatizada en casos individuales) dentro de los límites de tiempo legales.

5.2 Tratamiento de Datos
Axess se compromete al tratamiento de los datos personales solo en el marco de los contratos existentes y de conformidad con las instrucciones individuales del cliente. Si Axess se viera obligado a ceder los datos a terceros por imperativo legal, Axess informará al cliente sobre esa obligación legal de divulgar los datos. Cualquier otra transferencia de datos para fines ajenos a la relación contractual solo se podrá producir siguiendo instrucciones del cliente mediante solicitud por escrito.

Axess se asegurará de que todas las personas encargadas del tratamiento de datos queden sujetas a una obligación de confidencialidad antes del inicio de sus actividades - permaneciendo dicha confidencialidad en vigor incluso después de la finalización de sus actividades - o de que estén sujetas a una obligación legal adecuada de confidencialidad.

5.3 Deber de información
Axess prestará su apoyo al Cliente para cumplir con las obligaciones establecidas en los artículos 32 a 36 del RGPD (seguridad del tratamiento, notificación a la autoridad de control de violaciones relativas a datos personales, notificación de la persona afectada por una violación relativa a datos personales, evaluación del impacto en la protección de datos, consulta previa)

Previa solicitud, Axess proporcionará al Cliente toda la información necesaria (por ejemplo, certificaciones existentes, medidas técnicas y organizativas, etc.) que pruebe el cumplimiento de las obligaciones establecidas en el artículo 28 del RGPD (obligaciones del Encargado del Tratamiento). Además, Axess permitirá y aportará información durante las auditorías - incluidas las inspecciones -realizadas por el Cliente u otro auditor designado por el Cliente.

Axess informará al Cliente sin demora indebida en los casos de incumplimiento del RGPD o también si Axess considera que una instrucción del Cliente infringe la normativa sobre protección de datos de la Unión o de los Estados miembros.

5.4 Control de pedidos
Se garantiza que los datos personales objeto de tratamiento en nombre del cliente solo serán tratados de conformidad con las instrucciones del cliente. Axess mantiene contratos con terceros externos para los siguientes tipos de tratamiento de datos por encargo:
> Tratamiento de datos por parte de terceros externos
> Destrucción / eliminación de soportes de datos por parte de terceros externos
> Mantenimiento y mantenimiento remoto por parte de terceros externos
> Administración / administración remota por parte de terceros externos

El tratamiento de datos personales en nombre del cliente – siempre de conformidad con las instrucciones del cliente - quedará garantizado por las siguientes medidas:
> Instrucciones escritas
> Oferta y confirmación de pedido
> Seudonimización

5.5 Subgestores de datos
Axess está autorizado a utilizar subgestores de datos para el tratamiento de datos personales. Cualquier cambio previsto con respecto al subgestor de datos deberá notificarse al Cliente por escrito con antelación suficiente para que el Cliente pueda oponerse al cambio. Quedarán excluidas de esta regla las situaciones en las que la notificación no es posible o viable (especialmente en caso de peligro inminente). Axess celebrará un contrato por escrito con los subgestores de datos y acordará con ellos, haciendo los cambios pertinentes, las mismas obligaciones en virtud de la ley de protección de datos que las presentadas en este capítulo.
Los siguientes subprocesadores están contratados por Axess:
> Designa Axess Industries Holding con sus empresas afiliadas
> Axess AG con todas sus empresas afiliadas
> Designa Verkehrsleittechnik GmbH con todas sus empresas afiliadas
> Designa Digital Solutions GmbH
> Microsoft Corporation
> HubSpot, Inc.

En el caso de un contrato de compra con un revendedor oficial de Axess, Axess solo entregará datos al contratista respectivo (socio o revendedor).

6 Gestión de los datos contractuales a la terminación del contrato
Tras la terminación de las relaciones comerciales subyacentes, Axess devolverá todos los Datos personales al Cliente en un formato habitual del tratamiento de datos o los eliminará, a menos que exista la obligación de almacenar los Datos personales en virtud de la legislación de la Unión o de los Estados miembros.

7 Disposiciones finales
La presente Política de Seguridad tendrá la misma duración que la duración de la relación comercial entre Axess y el Cliente. En consecuencia, las disposiciones finales de ésta serán de aplicación al acuerdo para el tratamiento de los pedidos.