Medidas técnicas y organizativas conforme al artículo 32 del Reglamento General de Protección de Datos

Información sobre el documento	
Versión	1.0
Fecha	07/02/2019
Clasificación	Documento público
Estado de autorización	Aprobado
Versión original publicada por	Responsable de la Protección de Datos de IONOS
Versión actual publicada por	Responsable de la Protección de Datos del grupo United Internet AG
Publicado el	07/02/2019

A tener en cuenta

Este documento contiene información puesta a disposición de socios comerciales, clientes y otras partes externas que tienen un derecho legal u otro derecho de acceso justificado.

Preámbulo

La persona responsable ha aplicado medidas apropiadas de confidencialidad, integridad, disponibilidad y resistencia, así como procedimientos para la revisión y evaluación periódicas.

En la parte general se describen las medidas técnicas y organizativas que se aplicarán independientemente de los respectivos servicios, ubicaciones y clientes. En el anexo se describen las medidas que se aplicarán más allá de las documentadas en la parte general.

1. Confidencialidad

Confidencialidad es la propiedad de la información, por la que se garantiza que las personas, entidades o procesos no autorizados no tengan acceso a dicha información.

Control de entrada

- Personal de recepción y seguridad
- Autorizaciones de acceso (tarjetas, transpondedores y llaves) individuales, documentadas y dependientes de la función
- Tarjetas de acceso para empleados y pases para visitantes
- Los visitantes podrán estar dentro del edificio solamente acompañados por un empleado del personal interno.
- Sistema antirrobo
- Las oficinas quedan cerradas fuera del horario laborable.

Control de acceso: medidas técnicas

- Procedimientos formales para controlar la asignación de derechos
- Acceso sólo con nombre de usuario, contraseña y, en caso necesario, autenticación de dos factores
- Política de contraseñas forzada por el sistema
- Acceso a sistemas internos por conexiones remotas únicamente por una conexión VPN en dispositivos administrados por la persona responsable
- Mobile Device Management (gestión de dispositivos móviles)
- Cifrado de soportes de almacenamiento de datos
- Bloqueo automático de los ordenadores después de unos minutos de inactividad
- Política de escritorios limpios

Control de acceso: medidas organizativas

- Se crean registros de activos y se adoptan medidas sobre la base de la clasificación de datos.
- Uso de procedimientos criptográficos (p. ej., encriptación)
- Concesión de autorizaciones conforme al principio "need to know" (necesidad de conocer)
- Clasificación de los accesos conforme a roles y perfiles de los usuarios
- Registro de intentos de acceso
- Estaciones de trabajo de administrador
- El menor número posible de administradores (principio de mínimo privilegio)
- Destrucción de documentos

Seudonimización

- Si es posible o necesario, los datos personales se tratarán de forma anónima (disociación de los datos identificativos y almacenamiento en sistemas separados).

Control de separación

- Separación del entorno de desarrollo, ensayos y producción

- Los datos personales no pueden usarse en el entorno de ensayos.
- Arquitectura de tenencia múltiple / independencia lógica de datos en aplicaciones relevantes: bases de datos independientes, diferentes esquemas de bases de datos, conceptos de autorización y/o gestión de archivos estructurada

2. Integridad

La integridad de los datos personales se debe mantener siempre, mientras se conservan los datos personales actualizados, inalterados y completos en todo momento.

Control de transmisión

- Transmisión de datos a través de conexiones cifradas (p. ej., SFTP)
- Transmisión de datos personales conforme al principio "need to know"/"need to do" (necesidad de conocer)
- La información deberá clasificarse en función de la protección que requiera, de manera que la información confidencial y oficial se transmitirá solo por vías de comunicación seguras.
- Si es posible, encriptación de mensajes de correo electrónico
- Si es posible, transmisión de datos personales únicamente en forma seudonomizada o anonimizada
- Registro de la entrega de soportes de almacenamiento de datos físicos
- Entrega de documentos en papel que contengan datos personales en sobres opacos y sellados

Control de entrada

- Registro técnico de la introducción, modificación y eliminación de datos personales, así como control de los registros
- Trazabilidad de la introducción, modificación y eliminación de datos por nombres de usuario individuales (no por grupos de usuarios)
- Asignación de permisos (leer, escribir y eliminar) basada en roles
- Registro de los cambios administrativos

3. Disponibilidad y resiliencia

Los datos personales están disponibles y accesibles a los usuarios en todo momento.

- Uso de firewalls de hardware y software
- Sistemas de detección de intrusos
- Protección externa de sobretensiones y rayos
- Sistema de alimentación ininterrumpida (SAI)
- Manuales de emergencia para la recuperación de datos; protección contra la destrucción y pérdida accidental
- Pruebas de funcionamiento de copias de seguridad de datos
- Si es necesario, uso de sistemas redundantes (p. ej., RAID)
- Pruebas periódicas de las copias de seguridad de los datos
- Auditorías y pruebas de seguridad externas

4. Revisión y evaluación periódicas

¿Cómo se garantiza que las medidas de protección de datos mencionadas se revisen periódicamente?

Gestión de la política de privacidad

- Se han nombrado a un responsable de la protección de datos y un responsable de la seguridad de la información.
- Se ha establecido una organización de protección de datos y seguridad de la información.
- Cada empleado se compromete a mantener la confidencialidad de los datos personales.
- Los empleados están concienciados del manejo de los datos personales.
- Los nuevos empleados recibirán formación sobre el manejo de datos personales al incorporarse a la empresa.
- Se mantiene un registro de actividades de tratamiento y, en caso necesario, se realizan evaluaciones de impacto relativa a la protección de datos (EIPD).
- Se han establecido procedimientos para el ejercicio de los derechos de los interesados.

Control de encargo

- Los datos procesados en el marco de los contratos formalizados se tratarán exclusivamente según las instrucciones del cliente.
- Se selecciona cuidadosamente a los encargados en función de las medidas técnicas y organizativas a fin de proteger los datos personales.
- Las instrucciones sobre la manipulación de datos personales deberán constar por escrito.
- En caso necesario, podrá realizarse una transferencia de datos personales a un tercer país.

Protección de datos desde el diseño y por defecto

- Se garantiza que los sistemas y productos se desarrollen de manera que sean respetuosos de la intimidad.
- Solo serán objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Gestión de incidentes

- Existe un proceso documentado para detectar, registrar y documentar las infracciones de la protección de datos con la participación del responsable de la protección de datos.
- Existe un proceso de gestión de incidentes de seguridad con la participación del responsable de seguridad de la información.

Anexo 1: Medidas técnicas y organizativas específicas para los centros de datos

- Todos los centros de datos son certificados según la norma ISO 27001.
- Los sistemas de control de acceso supervisan y garantizan el acceso al centro de datos correspondiente únicamente al personal autorizado.
- Control de seguridad
- Videocámaras, detectores de movimiento y un sistema antirrobo vigilan el exterior del edificio.
- Áreas de acceso controlado
- Infraestructura de red altamente redundante
- Sensores de detección de humo e incendio conectado directamente al servicio de bomberos local
- Sistema de refrigeración en el centro de datos/la sala de servidores
- Control de humedad y temperatura en la sala de servidores
- No hay instalaciones sanitarias en o por encima de los centros de datos.
- Notificación de alarma en caso de acceso no autorizado a un centro de datos