Acuerdo de Procesamiento de Datos
Anexo 1: **Concepto de Protección de Datos**

Estado: Versión 2.5, 17.08.2023
Persona de contacto: Matthias Menne, Delegado de Protección de Datos de onOffice GmbH

Introducción

El Anexo 1 describe las medidas técnicas y organizativas según el Art. 32 del RGPD, que deben garantizar la seguridad de los siguientes procesamientos cubiertos por el contrato:

- Provisión de la solución de software CRM online onOffice enterprise
- Alojamiento de sitios web
- Importación de datos
- Transferencia de datos
- Alojamiento de correos electrónicos

Muchos de estos procesamientos se realizan en los mismos sistemas informáticos y bajo las mismas medidas de seguridad. Por lo tanto, al inicio de cada capítulo se describen estas medidas de seguridad comunes, y luego se abordan los procesamientos individuales.

Cifrado

El tráfico de red hacia y desde onOffice enterprise está asegurado mediante HTTPS. Se admiten las versiones TLS 1.0, 1.1 y 1.2. El certificado fue emitido por "GMO GlobalSign Inc", Portsmouth NH, EE. UU.

Los sitios web pueden estar asegurados mediante certificados verificados por la CA "Let's Encrypt", San Francisco CA, EE. UU.

Los soportes de datos enviados para importaciones de datos se cifran antes de ser devueltos al cliente.

Para el envío de correos electrónicos, se utiliza TLS con Perfect Forward Security, siempre que el servidor receptor lo admita.

Confidencialidad

La confidencialidad de los datos personales se garantiza permitiendo el acceso físico o lógico únicamente a personas autorizadas.

Control de Acceso (Físico)

Salvo que se indique lo contrario, todos los procesamientos se realizan en el centro de datos de Telehouse Deutschland GmbH (ver Anexo 2).

Este centro cuenta con control de acceso mediante un sistema de tarjetas sin contacto, vigilancia 24/7 por un servicio de seguridad y videovigilancia. La autorización de acceso a las salas de servidores se programa específicamente para cada sala.

Las copias de seguridad se almacenan en las instalaciones alquiladas por Telehouse Deutschland GmbH en el centro de datos de Equinix (Germany) GmbH en Düsseldorf.

Los empleados de ambos centros de datos no tienen acceso a los datos almacenados.

En las oficinas de onOffice GmbH en Aquisgrán, los datos personales del cliente solo se almacenan temporalmente y ya sea para pruebas de software internas (si es absolutamente necesario) o para importaciones de datos. La asignación de llaves a los empleados está regulada y documentada. Fuera del horario laboral, las oficinas están protegidas por un sistema de alarma, que notifica automáticamente a un servicio de seguridad en caso de alarma.

Los soportes de datos enviados en el marco de importaciones de datos se guardan de forma segura en las oficinas. La permanencia de los soportes de datos se documenta por escrito. Las importaciones de datos se realizan en un servidor ubicado en las oficinas de onOffice GmbH en Aquisgrán. El servidor se encuentra en una sala de servidores independiente, protegida por una alarma, registro de accesos y videovigilancia.

Control de Acceso (Credenciales)

El acceso a onOffice enterprise/smart solo es posible mediante la introducción del nombre del cliente correcto, el nombre de un usuario activo no bloqueado y la contraseña válida. El nombre de usuario y la contraseña no se muestran en texto claro al ingresarlos. La frecuencia con la que debe cambiarse una contraseña puede ser configurada por un usuario con derechos de administrador a través del software. La complejidad de una contraseña se verifica automáticamente al ingresarla; si no cumple con ciertos criterios, la contraseña no se acepta.

El acceso a los sistemas productivos está restringido al personal estrictamente necesario y asegurado mediante autenticación de clave pública-privada. Cuando un empleado de onOffice se da de baja, se eliminan sus accesos.

El software estándar instalado en los servidores se revisa regularmente para detectar actualizaciones críticas de seguridad. Estas actualizaciones se aplican tan pronto como sea posible sin comprometer la disponibilidad.

Los datos personales del cliente solo se procesan fuera de las oficinas de onOffice GmbH cuando es necesario, y se siguen las mismas directrices de seguridad informática que dentro de las oficinas.

El tráfico de red es supervisado por un firewall de hardware.

Control de Acceso a Datos

En onOffice enterprise/smart, el acceso a los datos se puede restringir por usuario. Para ello, los datos deben ser asignados a usuarios o grupos específicos y los derechos de los usuarios deben ser adecuadamente restringidos. Además, se puede contratar un módulo que permite configurar los permisos de lectura y escritura para registros individuales de direcciones / objetos / historiales para cada usuario. Los usuarios pueden crear una lista de los últimos registros abiertos por ellos.

Los buzones de correo en onOffice enterprise/smart se pueden asignar a uno o varios usuarios. El buzón ya no será visible para otros usuarios.

Integridad

Las modificaciones realizadas en los datos de contactos y propiedades en onOffice enterprise/smart se registran. Estas modificaciones pueden ser revisadas por usuarios con derechos de administrador.

onOffice enterprise/smart tiene múltiples versiones de clientes. Los datos de cada cliente se almacenan en una base de datos independiente. Un usuario no puede acceder a los datos de otros clientes sin iniciar sesión con el nombre del cliente, el nombre del usuario y la contraseña correspondientes.

Las modificaciones en la base de código de onOffice enterprise/smart se prueban cuidadosamente y se ponen a disposición de un grupo limitado de clientes durante unas semanas antes de su despliegue general. Las correcciones de errores se implementan para todos los clientes dos veces por semana, y en casos urgentes, de inmediato.

Los archivos adjuntos de correos electrónicos se verifican en busca de virus, y se está evaluando o ya se ha implementado la protección antivirus para otros procesamientos.

Disponibilidad

Las bases de datos de los clientes se respaldan cada noche mediante una copia de seguridad completa. Estas copias de seguridad se almacenan en las instalaciones alquiladas por Telehouse Deutschland GmbH en el centro de datos de Equinix (Germany) GmbH en Düsseldorf (ver Anexo 2). Los archivos de los clientes se respaldan una vez al mes mediante una copia de seguridad completa y cada noche mediante una copia de seguridad incremental.

Con excepción de “Importación de datos“ y “Transferencia de datos“, todos los procesamientos se realizan en el centro de datos de Telehouse. La disponibilidad de los datos está asegurada por una fuente de alimentación ininterrumpida redundante N+1, protección contra incendios con detectores de humo ópticos / térmicos y sistemas de extinción Inergen, así como conexiones de red redundantes a varios proveedores.

Para todos los procesamientos, hay suficiente capacidad de cálculo disponible para compensar la falla de varios servidores. Los datos de los clientes se almacenan en un sistema RAID5.

Para protegerse contra ataques DDoS, onOffice participa en la red Prolexic de Akamai. Todas las solicitudes a los sistemas de onOffice GmbH se enrutan a través de servidores de Akamai, filtrando las solicitudes que son parte de un ataque DDoS.

Legalidad del Procesamiento

Todos los empleados de onOffice GmbH están comprometidos con la confidencialidad de los datos y se les capacita en protección de datos y seguridad informática.

Con todos los subcontratistas se han firmado acuerdos de procesamiento de datos. Los subcontratistas son evaluados por su idoneidad antes de la firma del contrato. Esto garantiza que los empleados de los subcontratistas también estén obligados a mantener la confidencialidad.

En la planificación de funcionalidades y procesos, siempre se incorpora el principio de minimización de datos ("Privacy by Design").

Gestión de Protección de Datos

El concepto de protección de datos se implementa mediante instrucciones de trabajo, acuerdos y medidas técnico-organizativas. La idoneidad del concepto de protección de datos se revisa al menos anualmente. Si es necesario, se ajusta el concepto de protección de datos o su implementación.

Gestión de Respuesta a Incidentes

Los sistemas informáticos utilizados para los procesamientos se monitorizan continuamente. En caso de incidentes, el acceso a los datos personales se restaura lo más rápido posible. Después de los incidentes, se revisa si el concepto de seguridad informática o el plan de contingencia informática necesita ser revisado y si las medidas técnico-organizativas y la infraestructura informática son suficientes para evitar incidentes similares en el futuro.

Procesamiento de Datos en Países Terceros

onOffice utiliza la red Prolexic de Akamai. Para asegurar una protección óptima contra ataques DDoS, el tráfico hacia los sistemas de onOffice GmbH se enruta a través de servidores en todo el mundo. La supervisión del tráfico se realiza en los EE. UU. Por lo tanto, los siguientes datos personales pueden ser procesados fuera de la UE:

1. La dirección IP del cliente
2. El dominio que ha solicitado
3. En tráfico no asegurado por HTTPS: la URL

onOffice ha firmado las cláusulas contractuales estándar de la UE con Akamai en su versión de junio de 2021, utilizando el Módulo 3 (procesador y procesador).

Se ha realizado una revisión de la situación legal en los EE. UU. y un análisis de riesgos. No es necesario que el responsable tome más medidas de seguridad adicionales.