COSMO CONSULT
Business-Software für Menschen

MEDIDAS GENERALES DE PROTECCIÓN DE DATOS EN COSMO CONSULT

Versión: 3.0 | 22.03.2018

1 TABLA DE CONTENIDO

1. Medidas generales de protección de datos en COSMO CONSULT

Si los datos son tratados en nombre del responsable del tratamiento, el encargado del tratamiento no es una tercera parte en términos de la legislación en materia de protección de datos, y el responsable del tratamiento seguirá siendo responsable de la protección de datos en virtud de la ley de protección de datos externos.
El responsable del tratamiento está obligado, por tanto, a supervisar que el encargado del tratamiento de datos ponga en práctica las medidas técnicas y organizativas apropiadas y necesarias para cada tipo de tratamiento.
Este apéndice describe las medidas técnicas y organizativas adoptadas por el encargado del tratamiento para garantizar la aplicación de medidas técnicas y organizativas, de conformidad con el Artículo 32 del GDPR.
La descripción de las medidas concretas que se utilizan para proteger los datos tratados contra posibles abusos en relación con el propósito de protección y el tipo de datos.

1.1 COSMO CONSULT ha tomado medidas para garantizar la seguridad de objetos y datos, así como para el funcionamiento ininterrumpido de la instalación en términos de construcción, personal, organización y tecnología.

1.2 COSMO CONSULT se compromete a guardar secreto respecto de sus clientes.Todos los empleados de COSMO CONSULT se comprometen con la privacidad de los datos cuando son contratados.

1.3 En COSMO CONSULT, el alcance de la protección incluye cualquier manipulación de los datos de personas físicas o jurídicas y otros datos sensibles o confidenciales (p. ej. datos empresariales o financieros).

1.4 En todas las sedes y oficinas de COSMO CONSULT se han adoptado medidas de protección contra incendios y de prevención de siniestros.

1.5 En todas las ubicaciones se garantizan los requisitos para el control de accesos y de salida mediante la seguridad estructural de las oficinas y, por lo general, las áreas de seguridad están vigiladas por medios electrónicos. La eliminación de documentos confidenciales se lleva a cabo exclusivamente mediante un sistema de trituración o de destructoras de documentos.

1.6 COSMO CONSULT se basa en la tecnología más moderna de Microsoft, que cumple todos los requisitos en materia de protección de datos. Esto se evidencia gracias a los diversos sellos de protección de datos de los productos de Microsoft.

1.7 COSMO CONSULT emplea a varios especialistas en TI (que cuentan normalmente con la certificación Microsoft Certified) para comprobar las precauciones de seguridad, complementarlas conforme a los requisitos y desarrollarlas según las medidas técnicas más modernas.

1.8 COSMO CONSULT trata los datos durante la implementación de software, la migración de datos y con fines de evaluación. Por otra parte, COSMO CONSULT establece sistemas de prueba en coordinación con el cliente. Los sistemas de prueba se mantendrán durante el período de soporte de COSMO CONSULT o según lo acordado contractualmente. Previa consulta con el cliente, el conjunto de datos de los sistemas de prueba podrá ser un conjunto de datos ajustado para datos sensibles y simulados a efectos de las pruebas.

1.9 En el caso de mantenimiento remoto/acceso a los sistemas del cliente, siempre habrá un sistema de seguridad (medidas de cifrado, etc.) como protección contra el acceso no autorizado.

1.10 Como protección contra virus, todos los medios de comunicación, correos electrónicos y archivos adjuntos se analizan en busca de virus. Además, todos los PC y servidores están protegidos por el software Endpoint Protection gestionado de forma centralizada.

1.11 COSMO CONSULT ha migrado casi por completo los servicios centrales y los requisitos en materia de protección de datos a un centro de datos centralizado.

1.12 El tratamiento de los datos se lleva a cabo exclusivamente en el ámbito del GDPR de la UE.

1.13 Si se celebra un acuerdo de tratamiento de órdenes con nuestro cliente, se aplican las siguientes medidas adicionales de protección de datos:

1.13.1 El principio de separación de funciones existe en todas las áreas importantes. Las áreas afectadas por el tratamiento de datos están funcional y orgánicamente separadas. Todos los sistemas del cliente sólo son accesibles por los empleados autorizados, y por el respectivo equipo de proyecto o de soporte al cliente. Los derechos de acceso son asignados por el jefe de proyecto responsable y se verifican periódicamente.

1.13.2 En función de las necesidades del cliente, los datos de marcado para el mantenimiento remoto son personalizados, o solamente son accesibles por los empleados autorizados del respectivo equipo de proyecto o de soporte al cliente.

1.13.3 La protección y la seguridad de los datos tienen una gran importancia para COSMO CONSULT. Por esta razón, los procesos internos de COSMO CONSULT son auditados periódicamente.

2. Medidas técnicas y organizativas

2.1 Las medidas técnicas y organizativas (MTO) son medidas relativas a:

2.1.1 Control de órdenes, control de acceso físico, control de acceso lógico, control de acceso a datos, control de transmisión de datos, control de entradas, control de disponibilidad, control de separación y control de eficacia.

2.1.2 Tipo de intercambio de datos, suministro de datos, tipo y condiciones de tratamiento, retención de datos, así como el tipo y las condiciones de transmisión de datos.

2.1.3 Medidas para garantizar la confidencialidad, integridad, disponibilidad y estabilidad de los sistemas y servicios de manera permanente, así como la posibilidad de restaurar rápidamente la accesibilidad y disponibilidad de los datos personales en caso de un incidente técnico o físico.

2.1.4 Un procedimiento para la revisión, la evaluación y la validación periódica de la eficacia de estas medidas.

2.2 En tanto que determinados servicios sean alojados por los contratistas, COSMO CONSULT los seleccionará exclusivamente de acuerdo con las exigencias legales, los contratará por escrito e informará a los clientes en el contrato que se celebre sobre el pedido de tratamiento de datos.

2.3 El grupo COSMO CONSULT garantiza y asegura con carácter periódico el cumplimiento de las medidas técnicas y organizativas adoptadas por todas las empresas que se han sumado al Joint Controllership Agreement (Acuerdo de corresponsabilidad, en español), conforme al Artículo 26 del GDPR.

2.4 En general, las medidas técnicas y organizativas de COSMO CONSULT se basan en el progreso técnico y en desarrollos ulteriores. COSMO CONSULT tomará todas las medidas necesarias para aumentar la seguridad.
La documentación reciente sobre medidas técnicas y organizativas "Data Protection and Data security at COSMO CONSULT" (Protección y seguridad de datos en COSMO CONSULT, en español) está disponible para su descarga en el sitio web https://www.cosmoconsult.com/data-protection

2.5 Ubicaciones de tratamiento de datos

2.5.1 Centro de datos centralizado de COSMO CONSULT

COSMO CONSULT aloja todos los servicios y servidores centrales en Microsoft Azure

Véase https://azure.microsoft.com

2.5.2 Ubicaciones de COSMO CONSULT

COSMO CONSULT es un grupo internacional de empresas con varias sedes y lleva a cabo proyectos de TI en todo el mundo. Los reglamentos y medidas documentadas aquí se aplican a todas las sedes de la corresponsabilidad del tratamiento del grupo COSMO CONSULT.

Véase: https://www.cosmoconsult.com/data-protection

2.5.3 Tratamiento de datos en Microsoft Azure

En tanto que en el contexto de pedidos de clientes los datos son alojados en la plataforma Windows Azure y no se puede excluir la transmisión de datos personales fuera de Europa, se ha celebrado un contrato con Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublín 18, Irlanda, de acuerdo con las exigencias legales. La adecuación del nivel de protección de datos también está garantizada por una certificación válida actualmente, conforme a la denominada Privacy Shield (protección de privacidad, en español).

Más información:

https://www.privacyshield.gov/pmodalityicipant?id=a2zt0000000KzNaAAK&contact=true#dispute-resolution-1

2.6 Control de acceso físico

A continuación se describen las medidas que impiden la intrusión forzosa y no autorizada en las oficinas de COSMO CONSULT.

Las salas de servidores locales (en caso aplicable) están protegidas adicionalmente en todas las ubicaciones dentro de los edificios de oficinas.

2.6.1 Técnicas

modalidad	objetivo
Control de acceso físico	Sí
Sistema de bloqueo	Sí

2.6.2 Organizativas

Modalidad	objetivo
Registro de visitantes en recepción	Sí
Acompañamiento de visitantes personal/supervisado	Sí
Reglas sobre uso de llaves y registro de llaves (uso de llaves de seguridad)	Sí

2.7 Control de acceso lógico

COSMO CONSULTAR asegura el uso de los sistemas de tratamiento de datos mediante varios controles de acceso, de manera que sólo las personas autorizadas puedan acceder a ellos. Cada acceso requiere la identificación y autenticación del usuario. El acceso desde el exterior está protegido por un cortafuegos en todas las ubicaciones.

2.7.1 Técnicas

Modalidad	Objetivo
Autenticación con nombre de usuario y contraseña	Sí
Uso del software EndPoint Protection	Sí
Uso de cortafuegos	Sí
Uso de tecnología VPN	Sí
Cifrado de disco de datos interno (HD int.)	Sí
Cifrado de dispositivos externos (móviles) (memorias USB, HD, DVD ext., etc.)	Sí

2.7.2 Organizativas

Modalidad	Objetivo
Usuarios administrados y permisos de usuario	Sí
Asignación de contraseñas / Reglas para establecer contraseñas	Sí
Perfiles de usuario	Sí
Reglas sobre uso de llaves y registro de llaves (uso de llaves de seguridad)	Sí

2.8 Control de acceso a los datos

A continuación figuran las medidas de COSMO CONSULT para garantizar que las personas autorizadas a utilizar un sistema de tratamiento de datos sólo pueden acceder a los datos que se les proporcionan, y que los datos personales no pueden ser leídos, copiados, modificados o eliminados sin autorización durante el tratamiento, uso y después del almacenamiento.

2.8.1 Técnicas

Modalidad	Objetivo
Uso de destructoras de documentos o contenedores de recogida (sistema de eliminación de archivos)	Sí
Concepto de autorización	Sí

2.8.2 Organizativas

Modalidad	Objetivo
Concepto de autorización (grupos de AD, definición de roles)	Sí
Política de contraseñas, incluyendo longitud y modificación	Sí
Administración de derechos de usuario por administradores del sistema	Sí

2.9 Control de transmisión de datos

A continuación se exponen las medidas de COSMO CONSULT para garantizar que los datos personales no pueden ser leídos, copiados, modificados o eliminados sin autorización durante la transmisión electrónica o durante el transporte o el almacenamiento en portadores de datos, y que puede ser verificarse y determinarse adónde se transmitirán los datos personales.

2.9.1 Técnicas

Modalidad	Objetivo
Registro de transferencias de datos	Cliente
Túnel VPN (línea segura) hacia la red de COSMO CONSULT	Sí
Túnel VPN (línea segura) hacia la red del cliente	Cliente

2.9.2 Organizativas

Modalidad	Objetivo
Selección cuidadosa de empleados	Sí
Normas de uso para dispositivos externos (móviles)	Sí

2.10 Control de entradas

La siguiente es una lista de las medidas para garantizar que se puede verificar y determinar a posteriori si, y quién ha introducido, modificado o borrado datos personales en sistemas de tratamiento de datos.

2.10.1 Características especiales / notas

Con respecto al control de entradas, será el cliente quien deba implementar las MTO.

Por ejemplo, es responsabilidad del cliente asignar nombres de usuario individuales en lugar de nombres de inicio de sesión colectivos para grupos de empleados o equipos (p. ej. COSMO CONSULT; para prestar soporte al cliente) y registrar las entradas/modificaciones, etc. de datos, de modo que sea posible rastrear las entradas, modificaciones y eliminaciones de datos en el sistema de producción.

2.10.2 Técnicas

Modalidad	Objetivo
Registro de entradas, modificaciones y eliminaciones de datos (cambio de protocolo o similar).	Cliente

2.10.3 Organizativas

Modalidad	Objetivo
Asignación de derechos para introducir, modificar y eliminar datos de acuerdo con un concepto de autorización	Cliente
Trazabilidad de la introducción, modificación y eliminación de datos mediante nombres de usuario individuales (no grupos de usuarios)	Cliente

2.11 Control del pedido

A continuación se exponen las medidas de COSMO CONSULT para garantizar que los datos personales tratados en nombre de COSMO CONSULT por otros proveedores sólo pueden ser tratados de acuerdo con las instrucciones del cliente.

Una lista de sus subcontratistas aprobados se actualiza regularmente en https//www.cosmoconsult.com/data-protection. En el caso de un cambio, los clientes serán informados con antelación por correo electrónico.

2.11.1 Organizativas

Modalidad	Objetivo
Sólo en acuerdos por escrito de pedidos de tratamiento de datos	Sí
Sólo en acuerdos por escrito de acuerdos de pedidos de tratamiento	Sí
Selección del contratista desde el punto de vista de la diligencia debida (especialmente con respecto a la seguridad de los datos)	Sí
Obligación de los empleados del contratista de mantener la confidencialidad de los datos	Sí

2.12 Control de disponibilidad

A continuación se describen las medidas de COSMO CONSULT para garantizar que los datos personales están protegidos contra daños o pérdidas accidentales, o que pueden recuperarse rápidamente en caso de un incidente.

2.12.1 Características especiales / notas

Se deben realizar MTO con referencia al control de disponibilidad por parte de la parte compradora (cliente). Las MTO se utilizan exclusivamente para fines internos o propios de COSMO CONSULT y garantizan la aptitud para el trabajo y la accesibilidad.

2.12.2 Técnicas

Modalidad	Objetivo
Extintores de incendios en las salas de servidores locales (o en las proximidades)	Sí

2.12.3 Organizativas

Modalidad	Objetivo
Almacenamiento de datos de copias de seguridad en un lugar seguro	Sí
Precauciones de copia de seguridad y recuperación	Sí

2.13 Control de separación

Las siguientes medidas garantizan que los datos recopilados para fines distintos se pueden procesar por separado.

2.13.1 Técnicas

Modalidad	Objetivo
Separación entre sistemas productivos y sistemas de prueba	Sí
Separación entre bases de datos y entornos multiusuario	Sí

2.13.2 Organizativas

Modalidad	Objetivo
Definir derechos de acceso para diferentes clientes/consumidores	Sí

2.14 Control de eficacia

A continuación, se enumeran las medidas para asegurar que la organización interna de la empresa satisface las necesidades especiales de protección de datos.

2.14.1 Organizativas

Modalidad	Objetivo
Normas y regulaciones para la seguridad de TI	Sí
Normas y regulaciones para asegurar el inventario de datos	Sí
Manual de la organización en la ubicación	Sí
Auditorías periódicas para garantizar el cumplimiento de las MTO	Sí
Sesiones de formación regulares	Sí

3. Delegado de protección de datos

Marco Schröder

Datos de contacto:
2b Advice GmbH
Joseph-Schumpeter-Allee 25
53227 Bonn

Tel: +49 (228) 92 61 65 123
Fax: +49 (228) 92 61 65 109

Correo electrónico: cosmoconsult@2b-advice.com
Web: http://www.2b-advice.com