Autodeclaración sobre las medidas técnicas y organizativas para el tratamiento por encargo | Estado: 20.10.2021

De acuerdo con las disposiciones del Reglamento General de Protección de Datos de la UE (art. 28 de la RGPD), el cliente debe comprobar antes del inicio del tratamiento de datos si se han establecido en el contratista las medidas técnicas y organizativas adecuadas para proteger la confidencialidad, integridad, disponibilidad, resiliencia y recuperabilidad de los datos y si se - cumplen. El resultado de esta comprobación deberá documentarse. Para simplificar esta verificación, se proporciona la siguiente autodeclaración. Para una rápida legibilidad y una presentación transparente de las medidas, la autodeclaración está diseñada como una lista de control. Las medidas individuales apoyan varios objetivos de protección de datos del RGPD. Para evitar la repetición, las medidas se estructuran en función de sus objetivos. En general, las medidas cubren los objetivos de protección de datos del RGPD.

Las preguntas se refieren únicamente a los empleados y a los sistemas, procedimientos e instalaciones encargados o utilizados para la realización de los servicios u operaciones de tratamiento encargados.

Con el fin de poder proporcionar un tratamiento encargado seguro que cumpla con los requisitos de protección de datos, se han establecido las medidas técnicas y organizativas que se describen a continuación.

Solicite	Cumple con		Comentario / Explicación
	J	N	
1. información general			
¿Se ha nombrado un responsable de la protección de datos?	☑	☐	Thorsten Schröers SAFE-PORT Consulting GmbH datenschutz@trilux.com | privacy@safe-port.de
¿Recibe el responsable de la protección de datos formación periódica?	☑	☐	IHK Arnsberg / Sauerland ITKservice GmbH IQ-Zert GmbH & Co KG
¿Qué otro(s) cargo(s) desempeña el responsable de la protección de datos además de esta tarea?			No hay más actividad, como responsable externo de la protección de datos
¿Están los empleados obligados a mantener la confidencialidad de acuerdo con las disposiciones del GDPR?	☑	☐	Todos los empleados del Grupo TRILUX están obligados a mantener la confidencialidad y a observar la protección de datos de acuerdo con la RGPD y la BDSG.
¿Está el compromiso documentado de forma verificable?	☑	☐	Por escrito en el expediente personal
¿Se instruye continuamente a los empleados en los requisitos de la protección de datos y, en su caso, cómo?	☑	☐	Tipo de instrucción ☑ Formación en línea ☑ Instrucciones escritas ☑ Reuniones periódicas del equipo
¿Existe un concepto de supresión con una regulación de los periodos de retención o almacenamiento y para la supresión o destrucción oportuna y segura de los datos?	☑	☐	
¿Existe una gestión sistemática de la protección y la seguridad de los datos con un procedimiento regulado de revisión y evaluación?	☑	☐	

Solicite	Cumple con		Comentario / Explicación
	J	N	
¿Existe una certificación de seguridad informática o de gestión de la seguridad informática o cualquier otro certificado sobre la aplicación de la protección de datos en la empresa que cumpla la ley?	☑	☐	El tratamiento de datos se realiza en un centro de datos de un proveedor de la nube con sede en la UE. Está certificada según la norma DIN EN/ISO IEC 2700x y se somete a una rutina de inspección periódica.
¿Existe un concepto de protección de datos o un manual de protección de datos para regular y aplicar la protección de datos en la empresa?	☑	☐	
¿Existe un manual de seguridad informática o hay otras normas para las medidas técnicas y organizativas de protección de datos?	☑	☐	
¿Se utilizan subcontratistas?	☒	☐	
En su caso, ¿se imponen a los subcontratistas las mismas obligaciones que las establecidas entre el poder adjudicador y el contratista?	☑	☐	
¿Existen también los necesarios acuerdos u obligaciones de protección de datos con los proveedores de mantenimiento y otros servicios y, en caso afirmativo, de qué tipo?	☑	☐	Todos los proveedores de servicios están - obligados por escrito a cumplir la legislación vigente en materia de protección de datos.
¿El tratamiento de datos se lleva a cabo en el territorio de la República Federal de Alemania o en la Unión Europea o en los Estados del Espacio Económico Europeo?	☑	☐	

Solicite	Cumple con		Comentario / Explicación
	J	N	
2. medidas técnicas y organizativas			
2.1 Confidencialidad (Art. 32 párrafo 1 lit. b RGPD)			
2.1.1 Acceso a la empresa			
¿Están los locales y edificios protegidos contra el acceso no autorizado fuera del - horario de funcionamiento?	☑	☐	☑ Guardias de seguridad ☑ Detector de movimiento/sistema de alarma ☑ Sistema de control de acceso ☑ Sistema de cierre centralizado, cerraduras de seguridad
¿Están aseguradas las entradas y salidas?	☑	☐	Puertas de entrada al edificio ☑ Sí☐ No Puertas de escape/salidas de emergencia ☑ Sí☐ No☐ No se aplica Escaleras de incendios y escaleras ☑ Sí☐ No☐ No se aplica Entrega y zonas de entrega ☑ Sí☐ No☐ No se aplica
¿Está regulada la orientación y supervisión de los visitantes?	☑	☐	☑ Recepción ☑ Libro de visitas ☑ Placa de visitante ☑ Orientación personal de los visitantes
¿Se supervisa al personal externo, por ejemplo, al personal de mantenimiento y de servicio?	☑	☐	El personal de mantenimiento y servicio está supervisado en todo momento por un miembro del personal responsable del área correspondiente.

Solicite	Cumple con		Comentario / Explicación
	J	N	
¿Existen controles de acceso?	☑	☐	☑ Sistema de control de acceso ☑ con ☐ sin zonas de seguridad ☑ Sistema de cierre centralizado con mando a distancia Las autorizaciones de acceso sólo se conceden a un empleado si lo ha solicitado el respectivo supervisor y/o el departamento de RRHH. El principio de necesidad se tiene en cuenta a la hora de conceder las autorizaciones.
¿Están definidas las áreas de seguridad, por ejemplo, la sala de servidores, la centralita, los archivos, los distribuidores de red y protegidas por separado contra el acceso no autorizado?	☑	☐	
¿Están estas zonas de seguridad especialmente protegidas contra el acceso no autorizado?	☑	☐	Tipo de protección ☑ Sistema de control de acceso ☑ Sistema de cierre centralizado con Normativa clave
¿Las autorizaciones de acceso a estas zonas de seguridad están reguladas y documentadas en un concepto de autorización de acceso?	☑	☐	La asignación y gestión de claves se realiza - según un proceso definido que regula la concesión o retirada de autorizaciones de acceso a las salas tanto al inicio de una relación laboral como al final de la misma.
¿Existen otras medidas de protección para estas salas?	☑	☐	☑ Porter ☑ Sistema de alarma ☑ Tarjeta de la empresa

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.1.2 Acceso a los sistemas de procesamiento de datos			
¿Existen medidas para controlar el acceso al escritorio y a los sistemas en red?	☑	☐	Identificación segura del usuario ☑ Contraseña segura ☑Bloqueo de la contraseña después de 3 intentos fallidos Para acceder a los sistemas informáticos, los usuarios deben tener la autorización de acceso adecuada. Para ello, los administradores emiten las correspondientes autorizaciones de usuario. Sin embargo, esto sólo se hace si lo solicita el respectivo supervisor. La solicitud también puede hacerse a través del departamento de RRHH.
¿Existen reglas de contraseña para todos los niveles de acceso (red, servidor, aplicaciones) para garantizar una contraseña segura y confidencial?	☑	☐	El usuario recibe un nombre de usuario y una contraseña inicial, que debe cambiar la primera vez que se conecte. Las especificaciones de la contraseña incluyen una longitud mínima de 8 caracteres, por lo que la contraseña debe superar los requisitos de complejidad.
¿Se comprueba automáticamente el cumplimiento de estas normas en todos los niveles durante la entrada?	☑	☐	Las contraseñas se cambian regularmente. Se indica un cambio de contraseña automático. Se almacena un historial de contraseñas. Esto asegura que las últimas 10 contraseñas no puedan ser utilizadas de nuevo. Las contraseñas se almacenan siempre de forma encriptada.
¿Está configurado un circuito de pausa (salvapantallas) protegido por contraseña y con control de tiempo?	☑	☐	

Solicite	Cumple con		Comentario / Explicación
	J	N	
¿Están los sistemas protegidos contra la intrusión no autorizada y contra Internet?	☑	☐	☑ Cortafuegos ☑ Escáner de virus ☑ Separación de la red eléctrica Todos los sistemas de servidores y clientes están equipados con un software de protección antivirus que garantiza un suministro diario de actualizaciones de firmas. Todos los servidores están protegidos por cortafuegos a los que siempre se les da mantenimiento y se les proporcionan actualizaciones y parches. El acceso de los servidores y clientes a Internet y el acceso a estos sistemas a través de Internet también está protegido por cortafuegos. Esto también garantiza que sólo se puedan utilizar los puertos necesarios para la comunicación respectiva. Todos los demás puertos se bloquean en consecuencia.
¿Existen medidas de registro/seguimiento y, en su caso, cuáles?	☑	☐	☑ Configuración de usuarios y derechos ☑ Cambios en el sistema ☑ Intentos de acceso erróneos ☑ Control del sistema ☑ Inicio y fin de los procedimientos de procesamiento de datos
¿Se almacenan los datos de registro a prueba de auditorías y con protección de acceso?	☑	☐	
¿Se comprueban los datos de registro puntualmente y con regularidad en busca de acciones y procesos relevantes para la seguridad?	☑	☐	☑ Manual y de ocasión
¿Está el acceso a los sistemas de procesamiento de datos restringido por un sistema de derechos al grupo de usuarios requerido?	☑	☐	☐ Perfiles de derechos y gestión de derechos ☐ Limitación funcional de los terminales Las autorizaciones para los sistemas y aplicaciones informáticas son establecidas exclusivamente por los administradores.
¿Se ha asegurado el acceso de organismos externos y, en caso afirmativo, cómo?	☑	☐	☑ Conexión VPN ☑ Codificación ☑ Software especial para el mantenimiento y la asistencia a distancia

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.1.3 Protección de los datos contra el acceso no autorizado			
¿Existe un perfil de autorización documentado que garantice que cada empleado sólo tiene las autorizaciones de acceso que necesita para realizar sus tareas?	☑	☐	¿En qué forma? Si es necesario, también se diferencian según: ☑ Leer autorización ☑ Escribir el permiso Las autorizaciones se conceden siempre según el principio de necesidad de conocer. En consecuencia, sólo se conceden derechos de acceso a los datos, bases de datos o aplicaciones a las personas que mantienen y dan servicio a estos datos, aplicaciones o bases de datos o que participan en su desarrollo. Existe un concepto de autorización basado en roles con la posibilidad de asignar de forma diferenciada las autorizaciones de acceso, lo que garantiza que los empleados reciban los derechos de acceso a las aplicaciones y a los datos en función de su respectiva área de responsabilidad y, si es necesario, en base a un proyecto.
¿Existen medidas para limitar el almacenamiento, en particular la seudonimización o anonimización?	☑	☐	
¿Las autorizaciones definidas y sus cambios están documentados de forma comprensible?	☑	☐	
¿Se ha establecido un sistema de gestión de derechos para la asignación documentada de los mismos, que también garantice que los derechos que ya no son necesarios se cancelen rápidamente en caso de cambio en el área de responsabilidad?	☑	☐	El requisito previo es la correspondiente solicitud de autorización para un empleado por parte de un superior. Se ha establecido un proceso de salida correspondiente.
¿Existen otras medidas de control de acceso, si procede?	☑	☐	☑ Proceso de revisión y aprobación del programa ☑ Registro y evaluación de incidentes críticos para la seguridad

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.2 Integridad (Art. 32 párrafo 1 lit. b RGPD)			
2.2.1 Protección de los datos durante la transmisión y la transferencia			
¿Están los datos protegidos contra el acceso no autorizado durante la transmisión?	☑	☐	☑ Codificación ☑ Conexiones seguras, VPN
¿Están garantizadas la eliminación, la destrucción y el desecho de los soportes de datos?	☑	☐	Todo el personal tiene instrucciones de depositar la información que contenga datos personales y/o información sobre proyectos en los contenedores de destrucción designados.
¿Se contrata el borrado/destrucción de los soportes de datos a una empresa de servicios?	☑	☐	La destrucción de los soportes de datos y del papel la lleva a cabo un proveedor de servicios que garantiza la destrucción de acuerdo con la norma DIN 66399.
¿Existe un contrato/orden para ello de acuerdo con los requisitos del art. 28 de la RGPD?	☑	☐	
¿Está regulado el desmantelamiento seguro y confidencial de dispositivos con soportes de datos (por ejemplo, servidores, dispositivos multifuncionales, etc.)?	☑	☐	
En el caso del mantenimiento a distancia, ¿el acceso a los datos del cliente y a los sistemas del cliente se realiza únicamente a través de líneas seguras?	☑	☐	Asegurar las líneas: ☑ Encriptación VPN ☑ El acceso remoto a los sistemas informáticos se realiza siempre a través de conexiones cifradas.
¿Se garantiza una identificación/autenticación segura para el mantenimiento a distancia?	☑	☐	
En caso de mantenimiento a distancia, ¿se supervisan las líneas con dispositivos de seguridad adecuados, por ejemplo, registro y evaluación de registros?	☑	☐	

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.2.2 Control de las entradas de datos			
¿Se registran y controlan los procesos de marcación a los sistemas de los clientes de forma rastreable?	☑	☐	La introducción, la modificación y la supresión de los datos personales tratados por cuenta del cliente quedan siempre registradas. Los empleados están obligados a trabajar con sus propias cuentas en todo momento. Las cuentas de usuario no pueden ser compartidas o utilizadas conjuntamente con otras personas.
¿Se registran el uso de los sistemas de procesamiento de datos y la introducción de datos?	☑	☐	Registro del uso de los archivos: ☑ Sí☐ No Registro de entradas y cambios: ☑ Datos relacionados con el campo ☑ Registro relacionado con
¿Se han establecido autorizaciones de usuarios con perfiles de derechos diferenciados?	☑	☐	Derechos: ☑ Leer, modificar, borrar ☑ Acceso parcial a datos y funciones
¿Se ha establecido un procedimiento para la asignación comprensible de los derechos y para la modificación o cancelación de los mismos?	☑	☐	Las autorizaciones se conceden siempre según el principio de necesidad de conocer. En consecuencia, sólo se conceden derechos de acceso a los datos, bases de datos o aplicaciones a las personas que mantienen y dan servicio a estos datos, aplicaciones o bases de datos o que participan en su desarrollo. El requisito previo es la correspondiente solicitud de autorización para un empleado por parte de un superior. Se ha establecido un proceso de salida correspondiente.
¿Se respeta el principio de mínimos en la asignación de derechos?	☑	☐	
¿Están separados los organismos de asignación/autorización de derechos y los de establecimiento de derechos?	☑	☐	

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.2.3 Control de las operaciones de tratamiento			
¿Se supervisa la ejecución de la acción de pedido/servicio del cliente de forma rastreable para garantizar su finalización de acuerdo con el pedido?	☑	☐	Las normas correspondientes se encuentran en el contrato de tramitación por encargo.
¿Existen mecanismos adecuados de registro y evaluación para controlar el acceso no autorizado a los sistemas y datos de los clientes?	☑	☐	Las normas correspondientes se encuentran en el contrato de tramitación por encargo.
¿Existen normas sobre la gestión de incidentes y el cumplimiento de las obligaciones de notificación al cliente?	☑	☐	Las normas correspondientes se encuentran en el contrato de tramitación por encargo.
Cuando se adjudican contratos de servicios (por ejemplo, de servicios informáticos, de mantenimiento, etc.), ¿se respetan los requisitos del artículo 28 del RGPD?	☑	☐	☑ Selección del contratista ☑ Revisión de las medidas técnicas y organizativas del contratista ☑ Celebración de un contrato con arreglo al artículo 28 del RGPD ☑ Revisión periódica del contratista
¿Se supervisan y registran de forma fiable las actividades de mantenimiento de los sistemas de procesamiento encargados?	☑	☐	

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.3 Disponibilidad y resiliencia de los sistemas (art. 32 (1) (b) GDPR)			
2.3.1 Garantizar la disponibilidad de los datos			
¿Están los datos de los clientes protegidos contra la destrucción y la pérdida mediante procedimientos de copia de seguridad adecuados?	☑	☐	☑ Stock de datos reflejados ☑ Copias de seguridad periódicas/solución de respaldo ¿Existe un concepto de copia de seguridad que especifique la forma de realizar una copia de seguridad periódica y la reconstrucción de los datos? ☑ Sí☐ No
¿Se han tomado medidas para asegurar la sala de servidores y la infraestructura informática?	☑	☐	Los datos del cliente se alojan en un centro de datos certificado según la norma DIN EN/ISO IEC 2700x.

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.3.2 Separación de los distintos clientes			
¿Están los datos de los distintos clientes debidamente separados entre sí para garantizar un tratamiento independiente?	☑	☐	Tipo de separación: ☑ Separación de clientes

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.4 Procedimientos de revisión, valoración y evaluación periódicas			
¿Existe un sistema de gestión de la seguridad informática?	☑	☐	Los datos del cliente se alojan en un centro de datos certificado según la norma DIN EN/ISO IEC 2700x.
¿Se comprueba periódicamente la eficacia de las medidas técnicas y organizativas de la empresa de otra manera?	☑	☐	La gestión de la protección de datos está implementada. Existe una directriz sobre la protección y la seguridad de los datos, así como directrices para garantizar la aplicación de los objetivos de la directriz. Se ha creado un Equipo de Protección de Datos y Seguridad de la Información (DST) para planificar, aplicar, evaluar y ajustar las medidas de protección y seguridad de los datos. Las directrices se evalúan y adaptan periódicamente en cuanto a su eficacia. En particular, se garantiza que todos los empleados reconozcan los incidentes de protección de datos y los comuniquen inmediatamente a la DST. La DST investigará el incidente inmediatamente. Si los datos tratados por cuenta de clientes se ven afectados, se velará por informarles inmediatamente de la naturaleza y el alcance del incidente. En el caso del tratamiento de datos con fines propios, si se cumplen los requisitos del art. 33 del RGPD, se realizará una notificación a la autoridad de control en el plazo de 72 horas desde que se tenga conocimiento de la incidencia.

Solicite	Cumple con		Comentario / Explicación
	J	N	
2.5 Procedimientos de revisión, valoración y evaluación periódicas			
¿Se respetan los requisitos de "protección de datos por tecnología" y "configuración por defecto favorable a la protección de datos"? ("Privacidad por diseño" y "Privacidad por defecto")	☑	☐	Ya durante el desarrollo del software se procura que el principio de necesidad se tenga en cuenta en relación con las interfaces de usuario. Por ejemplo, los campos de los formularios y las máscaras de pantalla pueden diseñarse de forma flexible. Los campos obligatorios pueden ser proporcionados o los campos pueden ser desactivados. El software admite tanto el control de entrada mediante un registro de auditoría flexible y personalizable que proporciona un almacenamiento inmutable de los cambios en los datos y los permisos de los usuarios. Las autorizaciones sobre datos o aplicaciones pueden establecerse de forma flexible y granular.

Arnsberg | 20.10.2021

Lugar | Fecha

Firma