Selbstauskunft über technische und organisatorische Maßnahmen zur Auftragsverarbeitung | Stand: 20.10.2021

Nach den Vorschriften der EU-Datenschutzgrundverordnung (Art. 28 DSGVO) muss der Auftraggeber vor Beginn der Datenverarbeitung prüfen, ob beim Auftragnehmer geeignete technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit, der Integrität, Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit der Daten eingerichtet sind und eingehalten werden. Das Ergebnis dieser Prüfung ist zu dokumentieren. Zur Vereinfachung dieser Überprüfung wird die nachstehende Selbstauskunft erteilt. Zur schnellen Lesbarkeit und einer transparenten Darstellung der Maßnahmen ist die Selbstauskunft als Checkliste gestaltet. Einzelne Maßnahmen unterstützen mehrere Datenschutzziele der DSGVO. Um Wiederholungen zu vermeiden, werden deshalb die Maßnahmen nach ihren Maßnahmenzielen gegliedert. Insgesamt decken die Maßnahmen die Datenschutzziele der DSGVO ab.

Die Fragen beziehen sich nur auf Beschäftigte und Systeme, Verfahren und Einrichtungen, die mit der Durchführung der beauftragten Serviceleistungen bzw. Verarbeitungen betraut bzw. für diese Verarbeitungen eingesetzt werden.

Um eine sichere und datenschutzgerechte Auftragsverarbeitung leisten zu können, sind die nachstehend beschriebenen technischen und organisatorischen Maßnahmen eingerichtet.

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
1. Allgemeine Angaben			
Ist ein Datenschutzbeauftragter bestellt?	☑	☐	Thorsten Schröers SAFE-PORT Consulting GmbH datenschutz@trilux.com | privacy@safe-port.de
Unterzieht sich der Datenschutzbeauftragte einer regelmäßigen Fortbildung?	☑	☐	IHK Arnsberg / Sauerland ITKservice GmbH IQ-Zert GmbH & Co. KG
Welche Position/en bekleidet der Datenschutzbeauftragte neben dieser Aufgabe noch?			Keine weitere Tätigkeit, da externer Datenschutzbeauftragter
Sind die Beschäftigten auf die Wahrung der Vertraulichkeit nach den Vorschriften der DSGVO verpflichtet?	☑	☐	Alle Mitarbeiter der TRILUX-Gruppe werden zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes gem. DSGVO und BDSG verpflichtet.
Ist die Verpflichtung ist nachweisbar dokumentiert?	☑	☐	Schriftlich in der Personalakte
Werden die Mitarbeiter laufend in die Anforderungen des Datenschutzes eingewiesen, ggf. wie?	☑	☐	Art der Unterweisung ☑ Onlineschulungen ☑ Schriftliche Unterweisungen ☑ Regelmäßige Team-Meetings
Besteht ein Löschkonzept mit einer Regelung der Aufbewahrungs- bzw. Speicherfristen und zur fristgerechten und sicheren Löschung bzw. Vernichtung der Daten?	☑	☐	
Gibt es ein systematisches Datenschutz- und Datensicherheitsmanagement mit einem geregelten Verfahren zur Überprüfung und Evaluierung?	☑	☐	

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
Gibt es eine Zertifizierung zur IT-Sicherheit bzw. zum IT-Sicherheitsmanagement oder ein sonstiges Testat über eine gesetzeskonforme Umsetzung des Datenschutzes im Unternehmen?	☑	☐	Die Datenverarbeitung findet in einem Rechenzentrum eines in der EU-ansässigen Cloud-Anbieters statt. Dieser ist entsprechend DIN EN/ISO IEC 2700x zertifiziert und unterliegt einer regelmäßigen Überprüfungsroutine.
Gibt es ein Datenschutzkonzept bzw. ein Datenschutzhandbuch zur Regelung und Umsetzung des Datenschutzes im Unternehmen?	☑	☐	
Gibt es ein IT-Sicherheitshandbuch oder bestehen sonstige Regelungen für die technischen und organisatorischen Maßnahmen zum Datenschutz?	☑	☐	
Werden Unterauftragnehmer eingesetzt?	☒	☐	
Werden ggf. Unterauftragnehmern dieselben Verpflichtungen auferlegt, die zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind?	☑	☐	
Bestehen auch mit Wartungs- und sonstigen Dienstleistungsunternehmen die erforderlichen datenschutz-rechtlichen Vereinbarungen bzw. Verpflichtungen, ggf. in welcher Art?	☑	☐	Alle Dienstleister werden schriftlich auf die Einhaltung der aktuellen Datenschutzgesetze verpflichtet.
Wird die Datenverarbeitung auf dem Gebiet der Bundesrepublik Deutschland bzw. innerhalb der Europäischen Union oder der Staaten des Europäischen Wirtschaftsraums durchgeführt?	☑	☐	

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2. Technische und organisatorische Maßnahmen			
2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)			
2.1.1 Zutritt zum Unternehmen			
Sind Gelände und Gebäude außerhalb der Betriebszeit gegen unbefugten Zutritt gesichert?	☑	☐	☑ Wachpersonal ☑ Bewegungsmelder/Alarmanlage ☑ Zutrittskontrollsystem ☑ Zentrales Schließsystem, Sicherheitsschlösser
Sind Zu- und Ausgänge gesichert?	☑	☐	Gebäudeeingangstüren ☑ Ja ☐ Nein Fluchttüren/Notausgänge ☑ Ja ☐ Nein ☐ Entfällt Feuerleitern und -treppen ☑ Ja ☐ Nein ☐ Entfällt An- und Auslieferungsbereiche ☑ Ja ☐ Nein ☐ Entfällt
Ist die Führung und Beaufsichtigung von Besuchern geregelt?	☑	☐	☑ Empfang ☑ Besucherbuch ☑ Besucherausweis ☑ Persönliche Besucherführung
Wird Fremdpersonal, z. B. Wartungs- und Servicepersonal, beaufsichtigt?	☑	☐	Wartungs- und Servicepersonal wird, durch einen für den jeweiligen Bereich zuständigen Mitarbeiter, stets beaufsichtigt.

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
Sind Zutrittssicherungen eingerichtet?	☑	☐	☑ Zutrittskontrollsystem ☑ mit ☐ ohne Sicherheitszonen ☑ Zentrales Schließsystem mit Schlüssel-regelung Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.
Sind Sicherheitsbereiche definiert, z.B. Serverraum, TK-Anlage, Archive, Netzwerkverteiler und gegen unbefugten Zutritt gesondert geschützt?	☑	☐	
Sind diese Sicherheitsbereiche gegen unbefugten Zutritt besonders geschützt, ggf. wie?	☑	☐	Art des Schutzes ☑ Zutrittskontrollsystem ☑ Zentrales Schließsystem mit Schlüsselregelung
Sind die Zutrittsberechtigungen zu diesen Sicherheitsbereichen in einem Zutrittsberechtigungskonzept geregelt und dokumentiert?	☑	☐	Die Schlüsselvergabe und das Schlüssel-management erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.
Sind zu diesen Räumen sonstige Schutzmaßnahmen eingerichtet?	☑	☐	☑ Pförtner ☑ Alarmanlage ☑ Firmenausweis

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.1.2 Zugang zu den Datenverarbeitungssystemen			
Sind Maßnahmen zur Zugangskontrolle zum Desktop und zu den vernetzten Systemen eingerichtet?	☑	☐	Sichere Userkennung ☑ Sicheres Passwort ☑ Passwort-wiederholungssperre nach 3 Fehlversuchen Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung gestellt werden.
Bestehen für alle Zugriffsebenen (Netz, Server, Anwendungen) Passwortregeln zur Gewährleistung eines sicheren und vertraulichen Passworts?	☑	☐	Der Benutzer erhält einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort den Komplexitätsanforderungen bestehen muss.
Wird die Einhaltung dieser Regeln auf allen Ebenen bei der Eingabe automatisiert kontrolliert?	☑	☐	Passwörter werden regelmäßig gewechselt. Ein automatischer Passwortwechsel ist indiziert. Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können. Passwörter werden grundsätzlich verschlüsselt gespeichert.
Ist eine zeitgesteuerte passwortgeschützte Pausenschaltung (Bildschirmschoner) eingerichtet?	☑	☐	

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
Sind die Systeme gegen unbefugtes Eindringen und gegen das Internet geschützt?	☑	☐	☑ Firewall ☑ Virenscanner ☑ Netztrennung Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist. Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden. Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.
Sind Protokollierungen/Überwachungs-maßnahmen eingerichtet, ggf. welche?	☑	☐	☑ Einrichtung von Benutzern und Rechten ☑ Systemänderungen ☑ Fehlerhafte Zugriffsversuche ☑ Systemüberwachung ☑ An- und Abmeldung an Daten-verarbeitungsverfahren
Werden die Protokolldaten revisionssicher und zugriffsgeschützt gespeichert?	☑	☐	
Werden die Protokolldaten zeitnah und regelmäßig auf sicherheitsrelevante Aktionen und Vorgänge überprüft?	☑	☐	☑ Manuell und anlassbezogen
Ist der Zugang zu den Datenverarbeitungssystemen durch ein Rechtesystem auf den erforderlichen Nutzerkreis beschränkt?	☑	☐	☐ Rechteprofile und Rechteverwaltung ☐ Funktionelle Beschränkung von Endgeräten Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.
Ist der Zugang von externen Stellen aus sicher gestaltet, ggf. wie?	☑	☐	☑ VPN-Verbindung ☑ Verschlüsselung ☑ Spezielle Software bei Fernwartung/ Remoteunterstützung

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.1.3 Schutz der Daten vor unbefugtem Zugriff			
Besteht ein dokumentiertes Berechtigungsprofil, das sicherstellt, dass jeder Mitarbeiter nur über die Zugriffs-befugnisse verfügt, die er zur Aufgabenerledigung benötigt?	☑	☐	In welcher Form? Soweit erforderlich auch differenziert nach: ☑ Leseberechtigung ☑ Schreibberechtigung Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
Sind Maßnahmen zur Speicherbegrenzung, insbesondere zur Pseudonymisierung bzw. Anonymisierung eingerichtet?	☑	☐	
Sind die festgelegten Berechtigungen und deren Veränderungen nachvollziehbar dokumentiert?	☑	☐	
Ist eine Rechteverwaltung zur dokumentierten Rechtevergabe eingerichtet, die auch bei einer Veränderung des Aufgabengebiets eine zeitnahe Aufhebung nicht mehr benötigter Rechte sicherstellt?	☑	☐	Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Ein entsprechender Check-Out-Prozess ist eigerichtet.
Bestehen sonstige Maßnahmen zur Zugriffskontrolle, ggf. welche?	☑	☐	☑ Programmprüfungs- und Freigabeverfahren ☑ Protokollierung und Auswertung von sicherheitskritischen Vorfällen

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)			
2.2.1 Schutz der Daten bei Übertragung und Weitergabe			
Werden die Daten bei ihrer Übertragung vor unbefugter Kenntnisnahme geschützt?	☑	☐	☑ Verschlüsselung ☑ Sichere Verbindungen, VPN
Ist eine sichere Löschung, Vernichtung und Entsorgung von Datenträgern gewährleistet?	☑	☐	Alle Mitarbeiter sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.
Ist die Löschung/Vernichtung von Datenträgern an ein Dienstleistungs-unternehmen vergeben?	☑	☐	Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.
Besteht hierzu ein Vertrag/Auftrag nach den Vorgaben des Art. 28 DSGVO?	☑	☐	
Ist die sichere und vertrauliche Außerbetriebnahme von Geräten mit Datenträgern (z.B. Server, Multifunktions-geräte etc.) geregelt?	☑	☐	
Erfolgt bei Fernwartung der Zugriff auf die Kundendaten und Kundensysteme nur über sichere Leitungen?	☑	☐	Sicherung der Leitungen: ☑ VPN ☑ Verschlüsselung Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen.
Ist bei Fernwartung eine sichere Identifizierung/Authentifizierung gewährleistet?	☑	☐	
Werden bei Fernwartung die Leitungen durch geeignete Sicherheitseinrichtungen, z.B. Protokollierung und Protokoll-auswertung, überwacht?	☑	☐	

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.2.2 Kontrolle von Dateneingaben			
Werden die Einwahlvorgänge in Kundensysteme nachvollziehbar protokolliert und überwacht?	☑	☐	Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die im Auftrag verarbeitet werden, wird grundsätzlich protokolliert. Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.
Werden die Benutzung von Datenverarbeitungssystemen und die Eingabe von Daten protokolliert?	☑	☐	Protokollierung der Dateibenutzung: ☑ Ja ☐ Nein Protokollierung von Eingaben und Veränderungen: ☑ Datenfeldbezogen ☑ Datensatzbezogen
Sind Benutzerberechtigungen mit differenzierten Rechteprofilen eingerichtet?	☑	☐	Rechte: ☑ Lesen, ändern, löschen ☑ Teilzugriff auf Daten und Funktionen
Ist ein Verfahren zur nachvollziehbaren Rechtevergabe und Rechteänderung bzw. Rechteaufhebung eingerichtet?	☑	☐	Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Ein entsprechender Check-Out-Prozess ist eigerichtet.
Wird bei der Rechtevergabe das Minimalprinzip beachtet?	☑	☐	
Sind die Stellen zur Rechtezuteilung/ Rechtegenehmigung und Rechteeinrichtung getrennt?	☑	☐	

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.2.3 Kontrolle der Auftragsverarbeitungen			
Wird die Durchführung des Kunden-auftrags/der Serviceaktion nachvollziehbar überwacht, um eine auftragskonforme Erledigung zu gewährleisten?	☑	☐	Entsprechende Regelungen sind im Vertrag zur Auftragsverarbeitung zu finden.
Sind geeignete Protokollierungs- und Auswertungsmechanismen eingerichtet, um unzulässige Zugriffe auf Kundensysteme und Kundendaten zu überwachen?	☑	☐	Entsprechende Regelungen sind im Vertrag zur Auftragsverarbeitung zu finden.
Bestehen Regelungen zur Behandlung von Störfällen und zur Wahrnehmung der Meldepflichten an den Auftraggeber?	☑	☐	Entsprechende Regelungen sind im Vertrag zur Auftragsverarbeitung zu finden.
Werden bei einer Vergabe von Serviceaufträgen (z.B. IT-Service, Wartung, etc.) die Vorgaben des Art. 28 DSGVO beachtet?	☑	☐	☑ Auswahl des Auftragnehmers ☑ Überprüfung der technischen und organisatorischen Maßnahmen beim Auftragnehmer ☑ Abschluss eines Vertrags gemäß Art. 28 DSGVO ☑ Regelmäßige Überprüfung des Auftragnehmers
Werden Wartungstätigkeiten an Systemen zur Auftragsverarbeitung zuverlässig überwacht und protokoliert?	☑	☐	

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.3 Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)			
2.3.1 Gewährleistung der Verfügbarkeit der Daten			
Sind die Kundendaten durch geeignete Sicherungsverfahren vor Zerstörung und Verlust geschützt?	☑	☐	☑ Gespiegelter Datenbestand ☑ Regelmäßige Sicherungskopien/ Back-up-Lösung Gibt es ein Sicherungskonzept, in dem die Art und Weise einer regelmäßigen Sicherung und die Rekonstruktion der Daten festgelegt ist? ☑ Ja ☐ Nein
Sind Maßnahmen zur Sicherung des Serverraums und der IT-Infrastruktur eingerichtet?	☑	☐	Die Kundendaten sind in einem nach DIN EN/ISO IEC 2700x-zertifiziertem Rechenzentrum untergebracht.

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.3.2 Trennung verschiedener Mandanten			
Sind die Daten der verschiedenen Kunden in geeigneter Weise voneinander getrennt, um eine getrennte Verarbeitung zu gewährleisten?	☑	☐	Art der Trennung: ☑ Mandantentrennung

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung			
Ist ein IT-Sicherheitsmanagement-System in Betrieb?	☑	☐	Die Kundendaten sind in einem nach DIN EN/ISO IEC 2700x-zertifiziertem Rechenzentrum untergebracht.
Wird auf andere Weise zusätzlich regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen im Unternehmen geprüft?	☑	☐	Es ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird. Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst. Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden. Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

Anforderung	Erfüllt		Bemerkung / Erläuterung
	J	N	
2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung			
Werden die Anforderungen „Datenschutz durch Technik“ und „Datenschutz-freundliche Voreinstellungen“ beachtet? („Privacy by Design“ und „Privacy by Default“)	☑	☐	Es wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden. Die Software unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

Arnsberg | 20.10.2021

Ort | Datum

Unterschrift