Firma
SkySystems IT GmbH
Oeger Straße 47
58642 Iserlohn

Ansprechpartner:
R. Geitzenauer | S. Echtermann
Tel.: +49 2374 40948 0 | +49 2374 40948 0
E-Mail: r.geitzenauer@skysystems.it | s.echtermann@skysystems.it

Version	Datum	Autor	Änderungsgrund / Bemerkungen
1.0	05.06.2016	S. Katzorke	Erstausfertigung
1.1	24.05.2018	S. Katzorke	Änderung nach DSGVO
1.2	02.01.2019	S. Katzorke	Änderung der Firmierung SkySystems Datenschutz & Compliance GmbH
1.3	06.01.2020	S. Katzorke	Hinzufügen der Standorte Bochum und Schmallenberg
2.0	01.09.2020	S. Katzorke	Hinzufügen der elektronischen Zutrittskontrolle
2.1	25.05.2022	S.Echtermann	Löschen Standort Bochum/ Hinzufügen Standort Dortmund und Schuby
2.2	04.07.2022	S.Echtermann	Adressänderung Iserlohn

Inhaltsverzeichnis

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Die Büroräume der SkySystems IT GmbH befinden sich in einem Bürogebäude in Iserlohn sowie in einem Bürogebäude in Dortmund und Schmallenberg und Hamburg.

Die Zugänge zum Bürogebäude und auch zu den Büroräumen der SkySystems IT GmbH in Iserlohn sind Tag und Nacht verschlossen. Zugang zu den Büroräumen haben nur der Vermieter und die Mitarbeiter der SkySystems. Es kommt ein elektronisches und mechanisches Schließsystem zum Einsatz.
Die Zugänge zu den Büroräumen in Dortmund, Schmallenberg und Hamburg sind Tag und Nacht verschlossen. Zugang zu den Büroräumen haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein mechanisches Schließsystem zum Einsatz.
Dieses wird von der Personalabteilung der SkySystems IT GmbH verwaltet.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgen 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.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch einen Mitarbeiter Zutritt zu dem Bürogebäude und dann zu den Büroräumen. Die Eingangstür ist einsehbar und der Mitarbeiter, der die Eingangstür öffnet, trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet und einen Besucherausweis erhält.

Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die Büroräume der SkySystems IT GmbH in Iserlohn sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Zusätzlich ist ein Sicherheitsdienst mit dem Objektschutz beauftragt.

Die Büroräume der SkySystems IT GmbH in Dortmund sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Zusätzlich ist ein Sicherheitsdienst mit dem Objektschutz beauftragt.

Die Büroräume der SkySystems IT GmbH in Hamburg sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Zusätzlich ist ein Sicherheitsdienst mit dem Objektschutz beauftragt.

Die Büroräume der SkySystems IT GmbH in Schmallenberg sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Zusätzlich ist ein Sicherheitsdienst mit dem Objektschutz beauftragt.

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Für die Zugangskontrolle sind nachfolgende Maßnahmen von der SkySystems IT GmbH getroffen worden:

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.

Remote-Zugriffe auf IT-Systeme der SkySystems IT GmbH erfolgen stets über verschlüsselte Verbindungen sowie einer Zwei – Faktor - Authentifizierung.

Auf allen Server- und Client-Systemen der SkySystems IT GmbH ist eine aktuelle Virenschutzsoftware installiert, 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 erforderliche Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Darüber hinaus erfolgt eine automatische Sperrung nach einer zehnminütigen inaktiven Phase.

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Berechtigungen für IT-Systeme und Applikationen der SkySystems IT GmbH werden ausschließlich von Administratoren 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. Der Antrag kann auch bei der Personalabteilung gestellt werden.

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.

Alle Mitarbeiter der SkySystems IT GmbH sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Alle von der SkySystems IT GmbH für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

2. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Eine Pseudonymisierung der personenbezogenen Daten ist nicht möglich, da Kern des Produktes die Administration und Verwaltung der zur Verfügung gestellten / zu wartenden Systeme beinhaltet.

3. Integrität

3.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Eine Weitergabe von personenbezogenen Daten, die im Auftrag vom Kunden von der SkySystems IT GmbH erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistung für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei der SkySystems IT GmbH im Zusammenhang mit Kundenprojekten untersagt.

Mitarbeiter der SkySystems IT GmbH werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von der SkySystems IT GmbH 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.

4. Verfügbarkeit und Belastbarkeit

4.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Daten auf Serversystemen von der SkySystems IT GmbH werden mindestens täglich gesichert.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Alle Systeme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an die Administratoren auslöst.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1. Datenschutz-Maßnahmen

Bei der SkySystems IT GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

5.2. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.