Anlage

Technisch-organisatorische Maßnahmen

Version Februar 2019

Name/Anschrift des Auftragsverarbeiters/ Auftragnehmers:

Herr Romanus Lange
Indula Shopsystem GmbH
Auf den Steinen 2, 37191 Lindau / Harz

Der Auftragnehmer bestätigt für die folgenden gemachten Angaben die Richtigkeit.

Lindau, 19.02.19
Ort & Datum

Unterschrift des Auftragnehmers

Hinweis:

Bitte kreuzen Sie die Punkte in der letzten Spalte an, die für Ihr Unternehmen zutreffen.

Bei Änderungen der hier dokumentierten technischen – organisatorischen Sicherheitsmaßnahmen sind die Änderungen dem Auftraggeber unverzüglich mitzuteilen.

Diese TOM-Dokumentation ist dann entsprechend zu aktualisieren, mit dem aktuellen Tagesdatum zu versehen und durch Abstimmung mit dem Auftraggeber unter Ersetzung der Vorversion zum neuen Vertragsbestandteil zu machen.

Präambel

Der Auftragnehmer nutzt neben der eigenen Serverstruktur, die hier sicherheitstechnisch beschrieben ist, in einzelnen Bereichen das Rechenzentrum von Hetzner für die Datenspeicherung bzw. Datenverarbeitung im Bereich der personenbezogenen Daten.

Die Verantwortung zur datenschutz- und sicherheitskonformen Umsetzung für diese Strukturen liegt in der Verantwortung von Hetzner.

Hetzner ist zertifiziert nach ISO 27001. Zwischen dem Auftragnehmer und Hetzner ist eine Vereinbarung zur Auftragsverarbeitung vorhanden.

a. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

A.	**Serverseitig getroffene Zutrittskontrollmaßnahmen**	
01.01	Der/Die Server werden durch den Auftragnehmer selbst betrieben und befinden sich innerhalb des Unternehmens vom Auftragnehmer.	x
01.02	Der/Die Standort(e) des/der Server befinden sich am folgenden Ort (Angabe von Stockwerk und Gegebenheit des Raumes (z.B. fensterlos): OG1, nicht fensterlos	x
01.03	Der/Die Server ist/sind mittels einer Einbruchmeldeanlage (EMA) alarmgesichert.	x
01.04	Der Raum der/des Server(s) ist mit einem elektronischen Schließsystem versehen.	
01.05	Die Zutritte zum Raum werden nachvollziehbar gespeichert/protokolliert.	
01.06	Der Raum der/des Server(s) hat ein mechanisches Schloss. Die Ausgabe ist auf ein Minimum an Personen begrenzt, wird aber nicht protokolliert.	x
01.07	Die Zutrittsberechtigungen sind personenbezogen und auf ein Minimum vergeben.	x
01.08	Der Raum der/des Server(s) ist videoüberwacht. Die Bilddaten werden gespeichert.	
01.09	Betriebsfremde Personen werden zum Raum der/des Server(s) persönlich begleitet.	x
01.10	Der Raum der/des Server(s) dient weiteren Zwecken: Lagerung von Software	x
B.	**Clientseitig getroffene Zutrittskontrollmaßnahmen**	
01.11	Die Adresse der Clientarbeitsplätze ist identisch dem Ort der Serverinfrastruktur. *(Falls nein, bitte angeben)* zusätzlich weitere Home-Office-Arbeitsplätze	x
01.12	Das Bürogebäude des Firmensitzes ist teilweise umfriedet.	x
01.13	Ein Pförtnerdienst / besetzter Empfangsbereich innerhalb der Öffnungszeiten ist vorhanden.	x
01.14	Ein Besucherbuch wird geführt.	
01.15	Die Haupteingänge zu den Büroräumen sind mit einem elektronischen Schließsystem versehen.	x
01.16	Die Ausgabe der Schlüssel bzw. Chips/Karten wird protokolliert.	x
01.17	Der Eingangsbereich ist videoüberwacht. Die Bilddaten werden gespeichert.	

01.18	Die Büroräume sind alarmgesichert.	x
01.19	Sonstiges	

2. Zugangskontrolle

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

02.01	Ein persönlicher Passwort / Benutzername Zugangsschutz zu den Systemen ist vorhanden.	x
02.02	Für die Administration der Systeme ist ein eigenständiger ADMIN-Account vorhanden.	x
02.03	Es existieren verbindliche Passwortparameter im Unternehmen.	x
02.04	Das IT System zwingt den Nutzer zur Einhaltung der Passwort- Vorgaben.	x
02.05	Eine automatische passwortgeschützte Bildschirmsperre ist eingestellt.	x
02.06	Es existieren verbindliche Vorgaben zum manuellen Sperren des Clients.	x
02.07	Bei Verlust / Vergessen / Ausspähen eines Passwortes wird das Passwort umgehend geändert.	
02.08	Eine Begrenzung von Anmeldeversuchen ist vorhanden.	
02.09	Es existieren passwortgesicherte und verschlüsselte Fernzugänge	x
02.10	Die Systeme sind mit einer Firewall abgesichert. Die Firewall wird regelmäßig upgedatet.	x
02.11	Mobile Endgeräte und weitere Speichermedien sind verschlüsselt	x
02.12	Sonstiges	

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.

03.01	Es existiert ein differenzierendes Berechtigungskonzept.	x
03.02	Bedarfsgerechte Rechtevergabe bei Mitarbeitern	x
03.03	Eine Protokollierung der Zugriffe auf Daten findet statt.	
03.04	Es existieren getrennte Produktiv- und Testsysteme.	x
03.05	Nicht mehr benötigte Datenträger mit personenbezogenen Daten werden durch einen externen Dienstleister datenschutzkonform vernichtet.	
03.06	Nicht mehr benötigte Unterlagen mit personenbezogenen Daten werden durch einen externen Dienstleister datenschutzkonform vernichtet.	x
03.07	Sonstiges	

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

04.01	Die eingesetzten Verfahren sind mandantenfähig.	x
04.02	Je nach Funktion im Unternehmen existieren unterschiedliche Zugriffsrechte	x
04.03	Nutzung von Sandboxing-Verfahren *(Möglichkeit Programme in getrennten/gesicherten Containern auf den jeweiligen Geräten zu nutzen.)*	
04.04	Sonstiges	

5. Pseudonymisierung *(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)*

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:

05.01	Es existieren getrennte Produktiv- und Testsysteme.	x
05.02	.....	

b. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

6. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Über-tragung 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.

06.01	Schützenswerte personenbezogene digitale Daten werden bei ihrer Übertragung verschlüsselt bzw. per Passwort geschützt.	x
06.02	Mobile Endgeräte sind per PIN geschützt und verschlüsselt	x
06.03	Nutzung eines Virtual Private Network (VPN) für den Zugriff auf Daten	x
06.04	Nutzung einer elektronischen Signatur	
06.05	Sonstiges	

7. 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.

07.01	Zugriffe auf Daten werden protokolliert.	
07.02	Nutzung eines Dokumentenmanagementsystems	
07.03	Sonstiges	

c. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

8. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

A.	**Serverseitig getroffene Verfügbarkeitskontrollmaßnahmen**	
08.01	Der Serverraum verfügt über eine feuerfeste / feuerhemmende Zugangstür	
08.02	Der Serverraum ist mit Rauchmeldern/ Feuerlöschsystemen ausgestattet.	
08.03	Der Serverraum ist klimatisiert.	x
08.04	Der Serverraum verfügt über eine unterbrechungsfreie Stromversorgung.	x
08.05	Ein dokumentiertes Backup Konzept ist vorhanden.	
08.06	Die Funktionalität der Backup Wiederherstellung wird regelmäßig getestet.	x
08.07	Datensicherungen erfolgen regelmäßig.	x
08.08	Die Datensicherungen sind verschlüsselt.	x
08.09	Die Datensicherungen werden extern aufbewahrt (getrennter Brandabschnitt)	
B.	**Allgemeine Verfügbarkeitskontrollmaßnahmen**	
08.10	Die IT Systeme sind mit Virenschutz, Anti-Spyware, Spamfilter und Firewall geschützt.	x
08.11	Ein dokumentiertes Notfallkonzept bzw. Meldewegekonzept ist vorhanden.	x
08.12	Eine zügige Wiederherstellbarkeit des laufenden Betriebes ist möglich (Art. 32 Abs. 1 lit. c DS-GVO):	x
08.13	Sonstiges	

d. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

9. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

09.01	Das Unternehmen hat einen Datenschutzbeauftragten (DSB) bestellt:	x
09.02	Die Mitarbeiter werden regelmäßig im Datenschutzrecht geschult.	x
09.03	Die Mitarbeiter werden schriftlich auf das Datengeheimnis verpflichtet.	x
09.04	Dienstleister werden auf deren Qualifikation geachtet.	x

09.05	Mit Dienstleistern werden schriftliche Verträge geschlossen.	x
09.06	Mit Dienstleistern wird, sofern notwendig, eine ADV-Vereinbarung geschlossen.	x
09.07	Prüfung der TOM-Dokumentation (Technische und organisatorische Maßnahmen) des Auftragnehmers	x
9.08	Sonstiges	

10. Datenschutz-Management

Zentrale Verwaltung, Nachvollziehbarkeit und Protokollierung des aktuellen Datenschutzniveaus im Unternehmen

10.01	Nutzung eines Datenschutzmanagementsystems *(zentrale und strukturierte Ablage mit Nachweismöglichkeiten)*	x
10.02	Nutzung einer Datenschutzmanagementsoftware.	
10.03	Sonstiges	

11. Incident-Response-Management

Umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT/Datenschutz-Bereichen berücksichtigen.

11.01	Unterstützung von Sicherheitssoftware.	
11.02	Es sind Meldewege und Meldeprozesse bekannt.	x
11.03	Sonstiges	

12. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Einstellungen von Soft- und Hardware vor Nutzung und Herausgabe an Benutzer bzw. Kunden.

12.01	Beachtung bei der App-Entwicklung	x
12.02	Beachtung bei der Softwareprogrammierung	x
12.03	Beachtung bei der Einrichtung und Konfiguration von Systemen (Software und Hardware)	x
12.04	Sonstiges	