Anlage 1

Verpflichtende technische und organisatorische Maßnahmen (TOM) für Auftragsverarbeiter von Bizlearn gemäß der Datenschutz-Grundverordnung (DSGVO)

Stand: 19.05.2021

1. Auftragskontrolle

Sämtliche Mitarbeiter des Auftragsverarbeiters und der Sub-Auftragsverarbeiter sind schriftlich dem Datenschutz verpflichtet. Mit anderen Serviceanbietern und IT-Dienstleistern ist eine angemessene Vertraulichkeitsverpflichtung auf vertraglicher Basis vereinbart.

Bizlearn führt Kontrollen durch, um die Einhaltung der Verträge zwischen Auftragnehmer und Auftraggeber, sowie Sub-Auftragsverarbeitern oder Serviceanbietern und IT-Dienstleistern zu gewährleisten.

2. Dateneingabekontrolle

Es wird ausschließlich autorisierten und zum Datenschutz verpflichteten Personen der Zugriff auf personenbezogene Daten Betroffener erlaubt, im Rahmen ihrer Arbeitsaufgabe.

3. Datenintegritätskontrolle

Die betriebenen IT-Systeme und Infrastrukturen werden in Bezug auf Vertraulichkeitsrisiken zyklisch evaluiert und das Ergebnis der Evaluierung entsprechend berichtet.

Es wurde zum Schutz vor unautorisierten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt, wie folgt:

a) Dem Stand der Technik entsprechende IT-Sicherheitssysteme und -konzepte
b) Externe und interne Penetrationstests
c) Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Prüfer
d) Zertifizierung der IT-Systeme und Infrastrukturen
e) Standardisierte Verarbeitungsprozesse im IT-Betrieb

4. Datenübertragungskontrolle

Personenbezogene Daten Betroffener werden bei der externen Übermittlung mit demselben Schutzniveau wie bei einer internen Übermittlung geschützt.

5. Datenzugriffskontrolle

Es werden angemessene Sicherheitsmaßnahmen für die übertragenen personenbezogenen Daten zwischen dem Auftragnehmer und ihrem Auftraggeber im Rahmen der Vereinbarung festgelegt.

Die betriebenen IT-Systeme und Infrastrukturen werden in Bezug auf Vertraulichkeitsrisiken zyklisch evaluiert. Es wird eine Klassifikation von Daten durchgeführt. Personenbezogene Daten erhalten zumindest den gleichen Schutz wie „vertrauliche“ Informationen im Sinne der Datenklassifikation. Der Zugriff auf persönliche, vertrauliche oder sensible Informationen wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know“-Prinzip). Mit anderen Worten, Mitarbeitern oder Dienstleistern wird der Zugriff nur auf diejenigen Informationen gewährt, die sie zur Erledigung ihrer Arbeitsaufgabe benötigen.

Alle produktiven Serversysteme werden in Rechenzentren oder gleichwertig gesicherten Serverräumen betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung personenbezogener, vertraulicher und sonstiger sensibler Daten werden in regelmäßigen Abständen geprüft. Zu diesem Zweck werden interne und externe Sicherheits-überprüfungen und Penetrationstests durchgeführt.

Durch ein entsprechendes Löschkonzept wird die Löschung nicht mehr benötigter Daten geregelt. Die Installation nicht genehmigter eigener Software oder sonstiger Software ist nicht gestattet.

6. Systemzugriffskontrolle

Das Sicherheitspatch-Management gewährleistet die Anwendung entsprechender regelmäßiger Sicherheitsupdates. Die Gewährung des Zugriffs auf Systeme, zur Speicherung und Verarbeitung personenbezogener Daten, erfolgt mittels eines mehrstufigen Rollen- und Berechtigungssystems. Das Vergeben und Entziehen der Rollen werden durch einen sicheren und festgelegten Prozess geregelt. Alle Nutzer greifen über eine eigene eindeutige Benutzerkennung auf die Systeme zu. Gruppenberechtigungen sind nicht zulässig.

Das Unternehmensnetzwerk ist geschützt durch den Stand der Technik entsprechende Netzwerk-Sicherheitsmaßnahmen (Firewalls, Virenschutz etc.). Der Umgang mit Kennwörtern und deren Festlegung ist in einer Kennwortrichtlinie festgelegt. Die Weitergabe von Kennwörtern ist untersagt.

Alle Kennwörter haben die festgelegten Mindestbedingungen zu erfüllen und werden in verschlüsselter Form gespeichert. Im Fall von Domänenkennwörtern erzwingt das System mindestens alle sechs Monate eine Änderung des Kennworts, das den Anforderungen aus der Kennwortrichtlinie entsprechen muss. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner.

7. Trennungskontrolle

Es sind technische Möglichkeiten implementiert, um die Trennung von personenbezogenen Daten Betroffener zu ermöglichen.

8. Verfügbarkeitskontrolle

Es werden zyklisch die betriebenen IT-Systeme und Infrastrukturen in Bezug auf Verfügbarkeitsrisiken evaluiert.

9. Wiederstellungskontrolle

Bizlearn verfügt über entsprechende Datensicherungsverfahren, um geschäftskritische Verarbeitungen kurzfristig wiederherstellen zu können.

Daten werden entsprechend den festgelegten Zyklen gesichert und verwahrt. Die Aufbewahrung von Datensicherungen ist im Sinne eines Löschkonzepts und Löschzyklen harmonisiert.

10. Zutrittskontrolle

Das Gebäude wird durch angemessene Maßnahmen geschützt. Der Zutritt von Fremdpersonal in Rechenzentren erfolgt nur in Begleitung von autorisiertem Personal. Zu den Systemen und zur Infrastruktur der Rechenzentren hat ausschließlich autorisiertes Personal Zugang.

Die Vergabe der Zutrittsrechte an die berechtigten Personen erfolgt auf individueller Basis gemäß den Maßnahmen zur System- und Datenzugriffskontrolle. Gäste und Besucher in den Gebäuden müssen sich namentlich anmelden und von autorisierten Mitarbeitern begleitet werden. Das Gebäude ist durch den Stand der Technik und dem gebotenen Schutzbedarf entsprechend gesichert.