Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

der softstairs GmbH, Kippingstraße 24, 20144 Hamburg

1. ZUTRITTSKONTROLLE

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

- ☐ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☐ Lichtschranken / Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☐ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☐ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

2. ZUGANGSKONTROLLE

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

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☐ Gehäuseverriegelungen
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Einsatz von Intrustion-Detection-Systemen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☒ Einsatz von Anti-Viren-Software
- ☐ Einsatz einer Hardware-Firewall
- ☐ Erstellen von Benutzerprofilen
- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☐ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☒ Einsatz einer Software-Firewall

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.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Anzahl der Administratoren auf das „Notwendigste" reduziert
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☐ Verschlüsselung von Datenträgern
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- ☐ Protokollierung der Vernichtung

4. 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.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen-Abruf- und Übermittlungsvorgängen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

5. 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.

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
  AZUBI-PLANER
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

6. AUFTRAGSKONTROLLE

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

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ Vertragsstrafen bei Verstößen
- ☐ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. VERFÜGBARKEITSKONTROLLE

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

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Erstellen eines Backup- & Recoverykonzepts
- ☐ Erstellen eines Notfallplans
- ☐ Serverräume nicht unter sanitären Anlagen

8. TRENNUNGSGEBOT

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

- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☒ Festlegung von Datenbankrechten
- ☒ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☒ Trennung von Produktiv- und Testsystem

Hamburg, 01.02.2016
Datum

Herr Sebastian Tempel (Geschäftsführung)
Verantwortlicher für die Erstellung

Unterschrift des Verantwortlichen