Anhang 1 – zum Vertrag über Auftragsverarbeitung

Technisch-organisatorische Maßnahmen (Art 32 DSGVO)

(Version V1 – Stand 23.04.2018)

Abkürzungsverzeichnis:

HN = Hauptniederlassung von kapper.net (1090 Wien, Alserbachstraße 11).
VIVI1 = Serverzentrum am Standort 1010 Wien, Liebiggasse 9
VIVI2 = Serverzentrum am Standort 1010 Wien, Liebiggasse 8

INFORMATIONSSICHERHEIT

kapper.net hat eine interne Information Security Policy (ISecP) basierend auf der Norm ISO 27000ff eingeführt und auf den eigenen Systemen und auf den von kapper.net betreuten Kundensystemen („Managed Services"[1]) auf kapper.net Hardware umgesetzt.
Die ISecP beschreibt die sicherheitsrelevanten Anforderungen, welche für alle physikalischen Systeme und Teilsysteme, für deren einzelne Komponenten, für jede Art von Software, Daten und Informationen, für Strukturen und Prozesse, für die erforderliche Infrastruktur sowie für alle internen und externen Mitarbeiterinnen und Mitarbeiter sowie Funktionsträger gelten.

Kennzeichnung und sichere Verwahrung von Informationen → digitale Dokumente werden klassifiziert nach vertraulich, geheim, intern und öffentlich. Vertrauliche und geheime Dokumente werden entsprechend markiert und sind auch die Speicherorte nur vordefinierten Nutzern/MitarbeiterInnen zugänglich. Vertrauliche und geheime Informationen sind für Unbefugte unzugänglich aufbewahrt.

Sicherheit der Endgeräte → Alle Endgeräte verfügen über aktuelle Betriebssysteme und werden mit stets aktuellen Sicherheitsupdates versorgt. Es ist auf allen Geräten eine entsprechende Virenschutzsoftware installiert, welche aktuell gehalten wird. Allen Systemen ist eine aktive Firewall vorgeschaltet. Alle Endgeräte sind passwortgesichert, die Bildschirme werden bei Verlassen des Arbeitsplatzes gesperrt.

Passwörter → Geheimhaltung, Verbot der Offenlegung und der analogen schriftlichen sowie ungeschützten digitalen Dokumentation.

Teleworking und VPN → die externe Umgebung ist ausreichend geschützt, auch gegen „Shoulder Surfing", um unberechtigten Personen die Einsichtnahme zu verwehren.

Insbesondere sind die folgenden Maßnahmen am jeweiligen Standort umgesetzt:

1. VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

  HN → Zugangskontrollsystem (Sicherheitsschlüssel mit Schlüsselregelung, elektrische Türöffner, Videoüberwachung), Festlegung von Sicherheitszonen

  VIVI1 →Zugangskontrollsystem (Sicherheitsschlüssel mit Schlüsselregelung, Videoüberwachung, Protokollierung der Besucher), closed-shop-/closed-user-Betrieb (nur registrierte User haben Zutritt), Festlegung von Sicherheitszonen

[1] Als „Managed Service" wird eine Leistung von kapper.net bezeichnet, bei der durch den Zweck des Services und den spezifischen Auftrag des Auftraggebers an kapper.net die Übermittlung von, die Einsicht in bzw. der Zugriff auf personenbezogene Daten des Verantwortlichen durch kapper.net unumgänglich oder sehr wahrscheinlich sind.

KAPPER NETWORK-COMMUNICATIONS GmbH
A-1090 Wien, Alserbachstraße 11/6
https://kapper.net/
Tel. +43 [0]5 9080 0
Fax. +43 [0]1 3195502
email: info@kapper.net
HG Wien/Court of Commerce Vienna
FBNR/Registration No. 273960h
UID/VAT-ID: ATU62267148
UniCredit Bank Austria AG
IBAN: AT141100008615914200
BIC/SWIFT: BKAUATWW

VIVI2 → Zugangskontrollsystem (Sicherheitsschlüssel mit Schlüsselregelung, Magnet- oder Chipkarten, Protokollierung der Besucher), closed-shop-/closed-user-Betrieb (nur registrierte User haben Zutritt), Festlegung von Sicherheitszonen

- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung

  HN → Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Verschlüsselung von Datenträgern, Einsatz von VPN-Technologie

  VIVI1 → Schlüssel für Cages, Kennwörter (einschließlich entsprechender Policy), Sperrmechanismen, Verschlüsselung von Daten

  VIVI2 → Sicherheitsschlüssel für Cages, Kennwörter (einschließlich entsprechender Policy), Sperrmechanismen, Verschlüsselung von Daten

- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

  HN, VIVI1, VIVI2 → Standard-Berechtigungsprofile auf „need to know-Basis", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten

2. INTEGRITÄT[2]

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

  HN, VIVI1, VIVI2 → Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

  HN, VIVI1, VIVI2 → Protokollierung, Dokumentenmanagement

3. VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle** und **Wiederherstellbarkeit:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

  HN, VIVI1, VIVI2 → durch Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung, regelmäßige Updates der Systeme, Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

4. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- **Überprüfung der Einhaltung von Informationssicherheit:**

  HN, VIVI1, VIVI2 → Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen; Incident-Response-Management; datenschutzfreundliche Voreinstellungen

- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Verantwortlichen

  HN → eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Vorabüberzeugungspflicht, Nachkontrollen

[2] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

KAPPER NETWORK-COMMUNICATIONS GmbH
A-1090 Wien, Alserbachstraße 11/6
https://kapper.net/
Tel. +43 [0]5 9080 0
Fax. +43 [0]1 3195502
email: info@kapper.net
HG Wien/Court of Commerce Vienna
FBNR/Registration No. 273960h
UID/VAT-ID: ATU62267148
UniCredit Bank Austria AG
IBAN: AT141100008615914200
BIC/SWIFT: BKAUATWW