Anlage 1 Technische und organisatorische Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

- ☒ Alarmanlage
- ☒ Automatisches Zutrittskontrollsystem
- ☒ Schließsystem mit Codesperre
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungskräften
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung Serverraum
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Empfang

b) Zugangskontrolle: keine unbefugte Systemnutzung

- ☒ Zuordnung von Benutzerrechten
- ☒ Vorgaben für sichere Passwörter
- ☒ Authentifikation Benutzername / Passwort
- ☒ Bildschirmschoner
- ☒ Einsatz von individuellen Benutzernahmen
- ☒ Einsatz von VPN-Technologie (Fernzugriff)
- ☒ Einsatz von Intrusion-Detection-Systemen
- ☒ Zwei-Faktor-Authentifizierung

c) Zugriffskontrolle: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

- ☒ Berechtigungskonzept nach dem Need-to-know-Prinzip
- ☒ Nur notwendigste Administratoren
- ☒ Physische Löschung von Datenträgern
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern
- ☒ Verschlüsselung von Datenträgern
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz von Software-Firewall
- ☒ Rechteverwaltung
- ☒ Passwortrichtlinie
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ Ordnungsgemäße Vernichtung von Datenträgern (in Anlehnung an DIN 66399)
- ☒ Protokollierung der Vernichtung
- ☒ Einsatz von Anti-Viren-Software

d) Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

- ☒ Festlegung von Datenbank-Rechten
- ☒ Trennung von Produktiv- und Testsystem
- ☒ Logische Mandantentrennung (Software)
- ☒ Keine Produktivitätsdaten in Testsystemen

Klicken oder tippen Sie hier, um Text einzugeben.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

e) Weitergabekontrolle: kein unbefugtes Lesen, Kopieren oder Entfernen bei elektronischer Übertragung oder Transport

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☒ Nutzung sicherer Portal- und Ticketsystemlösungen
- ☒ E-Mail-Verschlüsselung

f) Eingabekontrolle: Feststellung, ob und von wem personenbezogene Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Z.B. Protokollierung, Dokumentenmanagement

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

g) Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO): Schutz gegen zufällige oder mutwillige Zerstörung sowie Verlust und Vorkehrungen, um möglichst schnell die Daten wiederherzustellen

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleiste in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Backup- und Recoverykonzept
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Serverräume nicht unter sanitären Anlagen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

h) Datenschutz-Management

- ☒ Datenschutzmanagementsystem
- ☒ Informationssicherheitsmanagementsystem
- ☒ Externer Datenschutzbeauftragter
- ☒ Regelmäßige Auditierung durch Interne (DSB und ISB) und Externe (v.a. TISAX)
- ☒ Informationssicherheitsbeauftragter
- ☒ Durchführung regelmäßiger Schulungs- und Sensibilisierungsmaßnahmen

Klicken oder tippen Sie hier, um Text einzugeben.

☒ Incident-Response-Management ☒ Notfallmanagement

i) Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung(Art. 25 Abs. 2 DSGVO)

☒ Beschränkung der Angaben und Verwendung auf das notwendige Maß ☒ Einhaltung von Branchenstandards

☒ Automatisierte Löschfunktionen für nicht mehr benötigte Daten ☒ Minimierung von Pflichtfeldern

j) Auftragskontrolle: Auftragsverarbeitung im Sinne von Art. 28 DSGVO

☒ Auswahl der (Unter-) Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☒ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z.B. über AVV) ☒ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf Vertraulichkeit

☒ Externer Datenschutzbeauftragter: Thomas Althammer, 0511-33060390, kontakt-dsb@althammer-kill.de

Mobiles Arbeiten

Mobiles Arbeiten beschreibt die arbeitsvertraglich vereinbarte Tätigkeit außerhalb der Betriebsstätte des Arbeitgebers. Sowohl ganztägiges als auch tagesanteiliges mobiles Arbeiten ist möglich. Nach Vereinbarung kann die Arbeit an verschiedenen Arbeitsorten und zu verschiedenen Tageszeiten innerhalb und außerhalb der Betriebsstätte geleistet werden. Unter mobilem Arbeiten versteht man die unter Zurverfügungstellung von mobilen Endgeräten eingeräumte Möglichkeit, die Arbeitsleistung an typischerweise wechselnden Orten außerhalb des Betriebs zu erbringen (etwa auf Reisen im Zug, im Hotel oder auf dem heimischen Sofa). Die Mitarbeiter*innen müssen nicht notwendig von zuhause arbeiten. Für den Schutz von Informationen & personenbezogenen Daten werden dabei folgende Standards eingehalten:

Jeder Benutzer hat sicherzustellen, dass jederzeit ein zu den Geschäftsräumen vergleichbares Sicherheitsniveau („Clean Desk“, Schutz vor Mithören und Einsichtnahme) vorhanden ist. Insbesondere müssen Informationen vor unberechtigten Dritten (Familienmitglieder, Mitbewohner) entsprechend ihrer Klassifizierung geschützt werden.

Ebenfalls muss vom Benutzer die verwendete Infrastruktur (z.B. Router/Internetverbindung) nach dem Stand der Technik abgesichert sein. Der Zugang zum Netzwerk der Organisation hat über eine von der Organisation bereitgestellte VPN-Verbindung zu erfolgen.

Die auf die jeweiligen Arbeitsverhältnisse anzuwendenden datenschutzrechtlichen Hinweise gelten gleichermaßen für das mobile Arbeiten.

Es wird ausdrücklich darauf hingewiesen, dass es den Mitarbeitenden untersagt ist, dienstliche Unterlagen mitzunehmen und außerhalb der Diensträume aufzubewahren.

Bei der Entsorgung von Dokumenten ist sicherzustellen, dass diese ordnungsgemäß vernichtet werden. Ist dies nicht möglich, so sind die Dokumente ordnungsgemäß in den Geschäftsräumen des Unternehmens zu entsorgen.

Mobile IT-Systeme müssen an einem sicheren Ort aufbewahrt werden, wenn sie längere Zeit unbeobachtet sind.