Technische und organisatorische Maßnahmen (TOMs) alphaben GmbH

Version	Datum	Autor	Kurzbeschreibung der Änderung / Änderungsgrund
0.9	26.06.2024	Marion Singler	Grundlegende Überarbeitung der TOMs
1.0	12.07.2024	Marion Singler	Erste freigegebene Version
1.1	13.10.2026	Florian Kriechbaumer	Klärung des Bezugs zum AVV Diverse Simplifizierungen und Klarstellung

I. Allgemeine Hinweise

1. Rechtlicher Hintergrund

Die EU-Datenschutzgrundverordnung (**DSGVO**) schreibt vor, dass jeder Verantwortliche sowie Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Als Teil der Erfüllung unserer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO dokumentieren wir die von uns gem. Art. 25 und 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen im Sinne § 7 des Auftragsverarbeitungsvertrags der alphaben GmbH. Gegenstand, Art und Zweck der Verarbeitung sowie die Datenarten und Kategorien betroffener Personen ergeben sich ausschließlich aus dem AVV.

2. Inhalt und Stand des Dokumentes

Unter Ziff. II. werden die technischen und organisatorischen Maßnahmen aufgeführt, die die alphaben GmbH (nachfolgend **„alphaben**“) in ihrem eigenen Kontrollbereich unmittelbar selbst umsetzt.

Hiervon abzugrenzen sind technische und organisatorischen Maßnahmen, die die von alphaben eingesetzten Dienstleister ihrerseits ergreifen, um für die von ihnen übernommenen Datenverarbeitungen ein angemessenes Schutzniveau zu gewährleisten.

Alphaben setzt zur Erbringung der vertraglichen Leistungen spezialisierte IT-Dienstleister ein.

Die für die Auftragsverarbeitung eingesetzten Unterauftragsverarbeiter sind in Anlage 4 des AVV aufgeführt. Ihre Einbindung und Kontrolle richten sich nach dem AVV.

II Technische und organisatorische Maßnahmen - alphaben GmbH

1. Vertraulichkeit (Art. 32 Abs.1 lit. b DSGVO, Art 5 Abs. 1 lit. f DSGVO)

Personenbezogene Daten müssen einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. alphaben hat geeignete technische und organisatorische Maßnahmen getroffen für den Schutz personenbezogener Daten

- vor unbefugter oder unrechtmäßiger Verarbeitung,
- vor unbeabsichtigtem Verlust,
- vor unbeabsichtigter Zerstörung und
- vor unbeabsichtigter Schädigung.

a. Zutrittskontrolle

Geeignete Maßnahmen der Zutrittskontrolle **verwehren unbefugten Personen physisch den Zutritt** zu Datenverarbeitungsanlagen. Sie stellen sicher, dass nur autorisierte Personen Zutritt zu den Datenverarbeitungsanlagen erhalten.

alphaben ergreift unter anderem die folgenden Maßnahmen, um den unbefugten Zutritt zu Datenverarbeitungsanlagen (insbes. Notebooks, Festplatten, IT-Server) zu sichern:

(1) Technische Maßnahmen

- Manuelles Schließsystem (z.B. Türschlösser)
- Automatisch zufallende und schließende Türen im Erdgeschoss
- Zusätzliches Zugangstor im Erdgeschoss

(2) Organisatorische Maßnahmen

- Schlüsselregelung und -dokumentation für Geschäftsräume
- Schließordnung (Regelung betreffend Öffnen und Verschließen von Gebäuden und Räumen)
- Besucherliste
- Besucher nur in Begleitung von Mitarbeitern
- Richtlinie/ Anweisung für Zutritt Externer
- Richtlinie/ Anweisungen für Umgang mit Besuch
- Sorgfältige Auswahl Reinigungspersonal (ohne eigenen Schlüssel für Geschäftsräume)

b. Zugangs- und Benutzerkontrolle

Die Zugangskontrolle soll die **unbefugte Nutzung von Datenverarbeitungssystemen verhindern**, so dass nur autorisierte Personen Zugang zu Datenverarbeitungssystemen erhalten und sie nutzen können.

alphaben ergreift diesbezüglich unter anderem folgende Maßnahmen:

(1) Technische Maßnahmen

- Einrichtung einer Multi-Faktor Authentifizierung
- Benutzer-Authentifikation (Name und Passwort)

- Einsatz einer spezifischen Passwort-Manager und -Sicherheitslösung zur Steigerung der (u.a.
- Passwort-) Sicherheit
- Passwortregelung über 1Password
- Regelmäßige Änderung von Passwörtern
- Sachkundiger Einsatz von Anti-Viren-Software (Avast)
- Sachkundiger Einsatz von Software-Firewalls (FritzBox mit interner Firewall)
- Sachkundiger Einsatz von Hardware-Firewalls (FritzBox mit interner Firewall)
- Einsatz von IP-Filtern (Real Site von Avast Virenschutz)
- Sperrung nicht erforderlicher Ports (erledigt durch FritzBox)
- Automatische Desktopsperre (nach spätestens 15 Minuten)
- Zugangssicherung des WLANs
- Weitere Sicherung des Firmennetzwerks durch Einrichtung eines gesonderten Gäste-WLANs
- Automatische Abmeldevorgänge bei Inaktivität des Mitarbeiters
- Automatische Aktualisierung der Betriebssysteme von Endgeräten durch regemäßige Updates/Patches
- Automatische Aktualisierung der Betriebssysteme in der unternehmensinternen IT-Infrastruktur (z.B. eigene Server, Router)
- Verschlüsselung von Datenträgern in Laptops/Notebooks und Mobiltelefonen

(2) Organisatorische Maßnahmen

Regelmäßige Überprüfungen und Schulungen intern

c. Zugriffs-, Daten und Speicherkontrolle

Zugriffskontrollmaßnahmen sollen gewährleisten, dass ein Benutzer des Datenverarbeitungssystems ausschließlich auf solche personenbezogenen Daten **Zugriff** erhält, zu deren Verarbeitung eine **Berechtigung** vorliegt.

alphaben ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb des Systems zu verhindern:

(1) Technische Maßnahmen

- Papierdokumente werden datenschutzkonform vernichtet
- Einsatz von Aktenvernichtern zur Vernichtung und Entsorgung von Akten (DIN 66399, Sicherheitsstufe 3 Partikelschnitt / „cross cut“)
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Änderungen an Dateien sind Personen zuordenbar
- Datenschutzkonforme Vernichtung von Endgeräten und Speichermedien durch eine Spezialfirma
- Physische Zerstörung von Datenträgern
- Die Vernichtung von Datenträgern findet kontrolliert mit Protokollierung statt
- Abschließbare Dokumentenschränke
- Automatische Aktualisierung der Betriebssysteme von Endgeräten durch regemäßige Updates/Patches
- Automatische Aktualisierung der Betriebssysteme in der unternehmensinternen IT-Infrastruktur (z.B. eigene Server, Router)

(2) Organisatorische Maßnahmen

Sorgfältige Vergabe von Zugriffsberechtigungen auf Basis eines bedarfsorientierten, differenzierten Berechtigungs- und Rollenkonzeptes

Berechtigungskonzept basiert auf dem Need-to-know-Prinzip

Zugriffsberechtigungen sind auf den minimal erforderlichen Personenkreis beschränkt und dienen rein zur administrativen Unterstützung

Zugriffe von Beschäftigten des Auftragsverarbeiters auf personenbezogene Daten erfolgen ausschließlich, soweit dies zur vertragsgemäßen Leistungserbringung, insbesondere für Betrieb, Wartung, IT-Sicherheit, Fehlerbehebung oder Support, erforderlich und von den dokumentierten Weisungen des Verantwortlichen umfasst ist. Die Zugriffsberechtigungen werden nach dem Need-to-know-Prinzip vergeben. Administrative Zugriffe sind auf besonders berechtigte Personen beschränkt.

- Formaler Prozess für Erteilung von Zugriffsberechtigungen
- Anzahl der Administratoren ist auf ein Mindestmaß reduziert
- Einsatz von Blickschutzfolien
- Interne Anweisung/Richtlinie zur Entsorgung von Papierdokumenten, Datenträgern und Endgeräten
- Vertraulichkeitsverpflichtung von Mitarbeitern
- Vertraulichkeitsverpflichtung von Reinigungspersonal

d. Trennungskontrolle (Sicherstellung der Trennung zu unterschiedlichen Zwecken erhobener Daten)

Maßnahmen der Trennungskontrolle sollen gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Verarbeitungszwecken erhoben wurden, **zweckgebunden und getrennt** verarbeitet werden. Außerdem gewährleistet die Trennungskontrolle die Mandantenfähigkeit der Verarbeitungsvorgänge, insoweit dies erforderlich ist (z.B. bei Nutzerkonten einer Online-Plattform).

alphaben ergreift unter anderem die folgenden Maßnahmen, um eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sicherzustellen:

(1) Technische Maßnahmen

- Wirksame, softwarebasierte Trennung unterschiedlicher Datenpools

(2) Organisatorische Maßnahmen

- Verwaltung von Benutzerberechtigungen für Datenbanken/ Anwendungen
- Verzeichnis von Verarbeitungstätigkeiten
- Anweisung zur Trennung privater und betrieblicher Daten
- Vertraulichkeitserklärungen

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO, Art 5 Abs. 1 lit. f DSGVO)

Personenbezogene Daten müssen einer Weise verarbeitet werden, die **eine angemessene Sicherheit** gewährleistet. alphaben hat geeignete technische und organisatorische Maßnahmen getroffen für den Schutz personenbezogener Daten

- vor unbefugter oder unrechtmäßiger Verarbeitung,

- vor unbeabsichtigtem Verlust, -
- vor unbeabsichtigter Zerstörung und -
- vor unbeabsichtigter Schädigung.

a. Weitergabekontrolle

Die Weitergabekontrolle verhindert, dass personenbezogene Daten bei der elektronischen **Übertragung** oder während ihres Transports oder ihrer Speicherung auf Datenträgern **unbefugt gelesen, kopiert, verändert oder entfernt** werden.

Außerdem wird im Rahmen der Weitergabekontrolle überprüfbar dokumentiert, welche Empfänger personenbezogene Daten erhalten dürfen.

alphaben ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten bei elektronischer Übertragung oder Transport zu verhindern:

(1) Technische Maßnahmen

- Automatische Aktualisierung der Betriebssysteme von Endgeräten durch regemäßige Updates/Patches
- Automatische Aktualisierung der Betriebssysteme in der unternehmensinternen IT-Infrastruktur (z.B. eigene Server, Router)
- Transportverschlüsselung mit TLS/SSL zur Sicherung der Datenübertragung zwischen App und Server
- Datenübermittlung von Schülerlisten der Schulen bei der Ersteinrichtung findet auf Basis einer Ende-zu-Ende-Verschlüsselungstechnologie über den spezialisierten Dienst von Tresorit statt
- Datenträger, die für Backup Zwecke genutzt werden, werden nicht auch zum Transport von Daten eingesetzt

(2) Organisatorische Maßnahmen

- Sorgfältige Auswahl von Dienstleistern
- Interne Anweisung/Richtlinie zur Entsorgung von Papierdokumenten, Datenträgern und Endgeräten
- Automatisierte Protokollierung von Abruf- und Übermittlungsvorgängen

b. Eingabekontrolle

Maßnahmen der **Eingabekontrolle** sollen gewährleisten, dass **nachträglich überprüft** und festgestellt werden kann, ob und wie personenbezogene Daten eingegeben, verändert oder entfernt worden sind, um die **Richtigkeit** und Integrität der personenbezogenen Daten sicherstellen zu können.

alphaben ergreift unter anderem die folgenden Maßnahmen, um festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

(1) Technische Maßnahmen

- Automatisches Protokollieren von Änderungen und Eingaben der Nutzer mit Zeitstempel
- Protokollieren für Dokumente
- Protokollieren von Änderungen und Eingaben der Nutzer von Löschvorgängen

3. Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

Art. 32 Abs. 1 lit. a DSGVO zeigt die **Verschlüsselung** von personenbezogenen Daten als **wichtige Maßnahme** zum Schutz der Sicherheit personenbezogener Daten auf. alphaben ergreift u.a. folgende Verschlüsselungsmaßnahmen:

(1) Technische Maßnahmen

- Verschlüsselung von Datenträgern in Laptops/Notebooks und Mobiltelefonen
- Transportverschlüsselung durch TLS/SSL zur Sicherung der Datenübertragung zwischen App uns Server
- Datenübermittlung von Schülerlisten der Schulen bei der Ersteinrichtung findet auf Basis einer Ende-zu-Ende-Verschlüsselungstechnologie über den spezialisierten Dienst von Tresorit statt
- Verschlüsselung von Back-Ups (TimeMachine und Synology)
- Passwörter liegen in verschlüsselter Form vor

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

Es wird gewährleistet, dass **personenbezogene Daten gegen Zerstörung, oder Verlust geschützt** sind.

alphaben ergreift unter anderem die folgenden Maßnahmen zum Schutz der Daten gegen zufällige Zerstörung bzw. Verlust:

(1) Technische Maßnahmen

- Feuerlöschgeräte und weitere Brandschutzmaßnahmen in den Geschäftsräumen
- Verbaute FI-Schalter im Geschäftsgebäude
- Digitalisieren von Dokumenten in Papierform
- Automatische Aktualisierung der Betriebssysteme von Endgeräten durch regemäßige Updates/Patches
- Automatische Aktualisierung der Betriebssysteme in der unternehmensinternen IT-Infrastruktur (z.B. eigene Server, Router)

(2) Organisatorische Maßnahmen

- Auslagerung der Datenserver an spezialisierte Anbieter mit hohem Sicherheitsstandard, redundanten Systemen und automatisierten Datensicherungen
- Notfallpläne inklusive festgelegter Meldewege beim IT-Dienstleister vorhanden

5. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Es wird sichergestellt, dass Daten nach Zwischenfällen **rasch wiederherstellbar** sind.

alphaben ergreift unter anderem die folgenden Maßnahmen, um eine Wiederherstellung von Daten zu ermöglichen:

(1) Technische Maßnahmen

- Automatisierte zyklische Durchführung von Backup-Routinen für Daten, die bei den spezialisierten IT-Dienstleistern vorgehalten werden
- Automatische Backups, indem alle Daten über OneDrive/Sharepoint mit Microsoft synchronisiert und in den Microsoft-Rechenzentren gesichert werden

(2) Organisatorische Maßnahmen

- Anweisung zur regelmäßigen Sicherung lokal gespeicherter Daten
- Regelmäßige Überprüfung der Wiederherstellbarkeit durch IT-Dienstleister
- Besonderer Schutz der Backup-Datenträger vor Diebstahl oder Zerstörung durch IT-Dienstleister
- Regelung des Einsatzes privater mobiler Datenträger

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

Es wurden insbesondere folgende Verfahren zur regelmäßigen **Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen eingerichtet.

a. Datenschutz-Management (Datenschutzgerechte Betriebsorganisation)

alphaben ergreift unter anderem die folgenden Maßnahmen, um die innerbetriebliche Organisation so zu gestalten, sodass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

(1) Technische Maßnahmen

- Einsatz einer spezifischen Passwort-Manager und -Sicherheitslösung zur Steigerung der Sicherheit
- Einfache Ausübung des Widerrufsrechts von Betroffenen durch technische Maßnahmen (z.B. Widerspruchs-Links auf Websites oder in Newsletter-E-Mails)
- Auslagerung zentraler Datenverarbeitung auf die Systeme spezialisierter IT-Dienstleister mit besonders hohen Sicherheitsstandards

(2) Organisatorische Maßnahmen

- Zentrale Dokumentation aller Verfahrensweisen, internen Vorgaben und sonstigen Regelungen zum Datenschutz bei der Geschäftsleitung Jährliche Schulung der MitarbeiterInnen im Datenschutz
- Regelmäßige Sensibilisierung der Beschäftigen bzgl. Datenschutz, insbes. zur Vermeidung von Cyberangriffen mittels Social-Engineerings
- Verpflichtungen von MitarbeiterInnen auf die Vertraulichkeit

- Bestellung eines/einer Datenschutzbeauftragten
- Intern sind Verantwortliche für Datensicherheit und die laufende Dokumentation der Verfahrensschritte definiert
- Jährliche Überprüfung technischer und organisatorischer Maßnahmen
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DSGVO), beispielsweise ist die Lesesoftware so konzipiert, dass die Anwendungsdaten von den Softwarenutzern nicht ohne Weiteres exportiert oder an Dritte übermittelt werden können und dass bei der Nutzung grundsätzlich keine Eingabe von Zusatzinformationen ermöglicht wird
- Löschkonzept ist vorhanden
- Eingesetzte Software ermöglicht die Löschung von Daten
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Datenschutzfreundliche Voreinstellungen bei verwendeter Software
- Soweit möglich und sinnvoll wird die Datenverarbeitung nicht selbst organisiert, sondern es erfolgt eine Auslagerung spezialisierte IT-Dienstleister mit hohen Sicherheitsstandards
- Regelmäßige Überprüfung, ob für alle Endgeräte die erforderlichen Updates und Patches der Betriebssysteme installiert wurden
- Regelmäßige Überprüfung, ob die Betriebssysteme von Geräten der unternehmensinternen IT-Infrastruktur (z.B. eigene Server, Router) auf dem neusten Stand sind
- Jede neue Hardware und Software durchläuft im Rahmen der Investitionsplanung ein Genehmigungsverfahren.

b. Auftragskontrolle

- alphaben ergreift unter anderem die folgenden Maßnahmen, um die **weisungsgemäße** Verarbeitung von Daten im Auftrag sicherzustellen:
- Sorgfältige Auswahl von Auftragsverarbeitern
- Prüfung der TOM jedes (weiteren) Auftragsverarbeiters
- Weisungen an Auftragsverarbeiter werden schriftlich/elektronisch dokumentiert
- Mit eingesetzten Auftragsverarbeitern wurden Vereinbarungen zur Auftragsverarbeitung (AVV) abgeschlossen
- Eine eindeutige Vertragsgestaltung zwischen Auftraggebern und Auftragnehmern zur Datenverarbeitung personenbezogener Daten ist erfolgt
- Regelungen zum Einsatz neuer Subunternehmer sind vorhanden
- Daten werden nach Beendigung des Auftrags beim Auftragsverarbeiter datenschutzkonform gelöscht
- Bei längerer Zusammenarbeit: Regelmäßige Überprüfung der Gewährleistung des vereinbarten Schutzniveaus bei Auftragsverarbeitern
- Intern sind Verantwortliche für die Auswahl und Kontrolle der Auftragsverarbeiter definiert.