Vereinbarung zur Auftragsverarbeitung (AV)

nach Art. 28 Datenschutzgrundverordnung (DSGVO)

zwischen

blink.it GmbH & Co. KG
Robert-Bosch-Straße 13
64293 Darmstadt

- nachfolgend "Auftragsverarbeiter" genannt - (alternativ Vertreter nach Art. 27 DSGVO)

und

Firma: _____

Straße: _____

PLZ & Ort: _____

- nachfolgend “Auftraggeber” genannt -

Präambel

Im Rahmen des zwischen den Parteien geschlossenen Vertrag über die Nutzung der blink.it Applikation (im Folgenden „Hauptvertrag“) datiert vom _____ wird der Auftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeiten. Die Regelungen dieser Vereinbarung finden auch Anwendung auf zukünftige gleichartige Leistungsbeschreibungen. Aus datenschutzrechtlicher Sicht handelt es sich um Auftragsverarbeitung (im Folgenden „AV“) gem. Art. 28 Datenschutzgrundverordnung (im Folgenden „DSGVO“). Bei der AV bleibt der Auftraggeber datenschutzrechtlich verantwortlich dafür, dass die personenbezogenen Daten entsprechend geschützt sind. Nach Art. 82 Abs. 4 DSGVO wird der Auftragsverarbeiter im Außenverhältnis gesamtschuldnerisch Mithaftender.
Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1. Gegenstand und Dauer der Vereinbarung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten von Mitarbeitern und/oder Kunden des Auftraggebers ausschließlich im Auftrag und nach Weisung des Auftraggebers. Der Leistungsinhalt insbesondere der Zweck der Datenverarbeitung wird im oben genannten Hauptvertrag konkretisiert.
2. Die Dauer der vorliegenden Vereinbarung zur Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrags.

3. Die Art der verwendeten personenbezogen Daten sind im wesentlichen:
    a. Vorname, Nachname, E-Mailadresse, Anrede des jeweiligen Nutzers
    b. Zeitstempel über:
        i. Erste Anmeldung
        ii. Jeweils erster Kursbesuch
        iii. Jeweils der Besuch von Inhalten
        iv. Kurs Absolvierung
    c. Abgegebene Antworten von Quizzen und Umfragen
    d. Kommentare zu Inhalten
4. Es werden keine besonderen Arten von personenbezogenen Daten (wie bspw. Gesundheit, Religion, Biometrische Daten etc.) gemäß (Artikel 9 DSGVO) verarbeitet.

2. Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung/-erhebung/-nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftragsverarbeiter unterstützt den Auftraggeber darin und leitet etwaige an ihn gerichtete Anfragen von Betroffenen unverzüglich weiter.
2. Der Auftraggeber ist nach Art. 28 Abs. 1 DSGVO verpflichtet, die Zuverlässigkeit des Auftragsverarbeiters vor Beginn der Verarbeitung und sodann regelmäßig zu überprüfen. Der Auftragsverarbeiter wird ihn dabei unterstützen.
3. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und in gesonderter, schriftlicher Leistungsbeschreibung bzw. Vertragsänderung festzuhalten.
4. Der Auftraggeber behält sich das Recht vor, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragsverarbeiter zu erteilen. Alle Ergänzungen werden dokumentiert und mündliche Weisungen werden unverzüglich schriftlich oder per E-Mail durch den Auftraggeber dokumentiert.
5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen entstehen, bleiben unberührt. Der Auftraggeber muss erwartete Mehraufwände vor Realisierung freigeben, es sei denn, es ist Gefahr im Verzug.
6. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder einen begründeten Verdacht feststellt.
7. Der Auftraggeber ist verpflichtet, alle erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiter vertraulich zu behandeln.

3. Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in einer getroffener Vereinbarung oder einer Weisung verlangt.
2. Der Auftragsverarbeiter verarbeitet die Daten **ausschließlich** in der Bundesrepublik Deutschland oder in Mitgliedsstaaten der EU. Das gilt auch für die Lokation von etwaigen Verarbeitungssystemen/ Rechenzentren.
3. Der Auftragsverarbeiter sichert die auftragsgemäße Verarbeitung von personenbezogenen Daten und die sorgfältige Abwicklung aller vereinbarten Maßnahmen zu. Er verwendet die zur Verarbeitung überlassenen Daten - ohne Wissen des Auftraggebers – für **keine** anderen als die in dieser Vereinbarung bestimmten Zwecke.
4. An den Auftragsverarbeiter gerichtete Anfragen Betroffener leitet dieser unverzüglich an den Auftraggeber weiter. Er unterstützt den Auftraggeber bei der fristgerechten Beantwortung und stellt proaktiv die notwendigen Informationen zur Information Betroffener nach Art. 12 ff. DSGVO zur Verfügung.
5. Dem Auftragsverarbeiter ist bekannt, dass nach. Art. 33 f. DSGVO strafbewehrte Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind Vorfälle in jeglicher Art und Weise von unrechtmäßiger Übermittlung oder Kenntniserlangung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei gegen den Auftragsverarbeiter eingeleiteten Ermittlungen von Straf- oder Aufsichtsbehörden. Der Auftragsverarbeiter hat unverzüglich angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.
6. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Sofern der vermutete Verstoß schriftlich zur Kenntnis gebracht wurde, ist der Auftragsverarbeiter berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Dies gilt auch für etwaige Subunternehmer.
7. Der Auftragsverarbeiter wird den Auftraggeber, dessen Aufsichtsbehörden oder einen vom Auftraggeber bestellten Dritten jederzeit im Rahmen des Zumutbaren bei der Durchführung von Kontrollen bezüglich der Einhaltung der Vorschriften über den Datenschutz und die vertraglichen Vereinbarungen unterstützen, z.B. durch Bereitstellung geeigneter Dokumentation oder Nachweise der Einhaltung geeigneter Verhaltensregeln nach Art. 40 DSGVO, einschlägiger Zertifizierungen nach Art. 42 DSGVO oder anderer Prüfberichte. Der Auftraggeber ist grundsätzlich nicht berechtigt, Zugang zu den Räumlichkeiten (Rechenzenturm) auf denen die blink.it App betrieben wird und die Daten gespeichert werden zu

verlangen (siehe Fußnote[1]). Zur Überprüfung des Datenschutzes und Sicherheit des Rechenzentrums werden Zertifizierungen von unabhängigen Prüfstellen vorgelegt (ISO 27001 & BSI C5 Zertifizierung siehe hierzu: https://aws.amazon.com/de/compliance/programs/).

8. Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen nach vorheriger Abstimmung datenschutzgerecht zu vernichten bzw. zu löschen.
9. Zum Empfang von Weisungen des Auftraggebers befugte Personen sind: Herr Michael Witzke, m.witzke@blink.it, 06151 - 3921699. Christopher Hutz, privacy@blink.it, 06151 - 3921690. Für den Fall, dass sich die empfangsberechtigten Personen beim Auftragsverarbeiter ändern, wird der Auftraggeber dies dem Auftragsverarbeiter schriftlich oder in Textform mitteilen.

4. Subunternehmer

1. Die Beauftragung von Subunternehmern ist zugelassen, sofern der Auftragsverarbeiter dem Subunternehmer dieselben Datenschutzpflichten auferlegt, wie sie zwischen dem Auftraggeber und dem Auftragsverarbeiter vereinbart wurden und der Auftragsverarbeiter deren Einhaltung regelmäßig kontrolliert und das Ergebnis der Kontrollen dokumentiert.
2. Der Auftragsverarbeiter hält eine Liste der an der Auftragsverarbeitung für den Auftraggeber beteiligten bzw. auf dessen Daten zugriffsberechtigten Subunternehmer zum Abruf durch den Auftraggeber bereit. Die bei Abschluss dieser Vereinbarung beschäftigten Subunternehmer sind in **Anlage 2** (Subunternehmer) zu dokumentiert und gelten als genehmigt. Über neue Subunternehmer, die Zugriff auf Datenbestände des Auftraggebers erhalten, informiert der Auftragsverarbeiter den Auftraggeber mit einer Vorlaufzeit, die es diesem ermöglicht, dagegen Widerspruch einzulegen. Im Falle eines Widerspruchs, hat der Auftragsverarbeiter die Möglichkeit, das Vertragsverhältnis zum nächstmöglichen Termin einvernehmlich zu beenden.

5. Datenschutz und Sicherheit der Verarbeitung

1. Der Auftragsverarbeiter hält die gesetzlichen Regelungen nach Art. 28-33 DSGVO ein und unterstützt den Auftraggeber bei der Einhaltung der Art. 32-36 DSGVO soweit zumutbar. Sofern er nach Art. 38 DSGVO dazu verpflichtet ist, einen Datenschutzbeauftragten zu benennen, teilt er die Kontaktdaten – insbes. auch im Fall eines Wechsels – dem Auftraggeber mit.
2. Der Auftragsverarbeiter darf nur solche Beschäftigten den Zugang zu personenbezogenen Daten des Auftraggebers gewähren, die eine Vertraulichkeitsvereinbarung hinsichtlich personenbezogener Daten unterzeichnet haben sowie regelmäßig hinsichtlich der Bestimmungen des Datenschutzes geschult werden.

[1] blink.it selbst hat auch keinen Zugang zum Rechenzenturm. Dies ist auch sinnvoll, da das persönliche Kontroll-Recht wiederum ein Sicherheitsrisiko darstellen würde. Deshalb wird dieses Recht von unabhängigen Prüfstellen wahrgenommen. Siehe hierzu: https://aws.amazon.com/de/compliance/programs/

3. Auskünfte darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

6. Datensicherheitsmaßnahmen Art. 28 Abs. 3 c), Art. 32 DSGVO (s. auch Anlage 1)

1. Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet und dokumentiert die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen und stellt diese Dokumentation dem Auftraggeber auf Anforderung zur Verfügung, um den Anforderungen des Art. 5 DSGVO gerecht zu werden.
2. Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt. Sie sollen den Schutzzielen der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Systeme angemessen im Hinblick auf Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen Rechnung tragen. Insbesondere sollten auf Maßnahmen ergriffen werden, Verletzungen der Schutzziele schnellstmöglich zu erkennen. Die beschriebenen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und der angewandten Verfahren sind mit dem Auftraggeber abzustimmen.
3. Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftraggeber den Auftragsverarbeiter. Eine einvernehmliche Regelung über etwaige Mehraufwände zur Erfüllung der Anforderungen bleibt unberührt.

7. Haftung

1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Auftragsverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragsverarbeiter bei Verstoß gegen diese Vereinbarung vorbehalten. Aufgrund der gesamtschuldnerischen Haftung auch des Auftragsverarbeiters nach Art. 82 DSGVO bei rechtswidriger Datenverarbeitung sichert der Auftraggeber zu, den Auftragsverarbeiter hinsichtlich dieser Haftung sowie in Bezug auf die Verteidigung gegen solche Ansprüche schadlos zu stellen, sofern nicht ein Verstoß dessen gegen diese Vereinbarung vorliegt, unabhängig davon, ob die Verarbeitung tatsächlich rechtswidrig ist.
2. Wird der Auftragsverarbeiter über eine Rechtswidrigkeit der Verarbeitung von dritter Seite in Kenntnis gesetzt, so teilt er dies dem Auftraggeber unverzüglich mit. Entsteht die Rechtswidrigkeit nicht durch fehlerhafte Verarbeitung durch

den Auftragsverarbeiter und sorgt der Auftraggeber nicht umgehend für Abhilfe, so hat der Auftragsverarbeiter ein außerordentliches Sonderkündigungsrecht.

8. Sonstiges

1. Sollte das Eigentum des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen.
2. Für Nebenabreden ist die Schriftform erforderlich, das gilt auch für die Streichung der Schriftformklausel.
3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Auftraggeber und Auftragsverarbeiter verpflichten sich zu einer zulässigen Lösung, die dem wirtschaftlichen Ergebnis der unwirksamen Regel am nächsten kommt.

9. Annahmeerklärung

Zustimmung von Auftragsverarbeiter	Annahme von Auftraggeber
blink.it GmbH & Co. KG Durch:	Durch:
Ort, Datum & Unterschrift	Ort, Datum & Unterschrift

Anlage 1: Technisch & Organisatorische Schutzmaßnahmen (TOMs) nach Art. 32 DSGVO

Diese Anlage konkretisiert die getroffenen technischen und organisatorischen Schutzmaßnahmen, die sich aus einem Vertrag in seinen Einzelheiten beschriebenen Datenverarbeitung ergeben.

Diese Anlage findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen oder sonstigen Daten des Auftraggebers in Berührung kommen können.

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

(1) Schutzmaßnahmen der **Zutrittskontrolle:**
Maßnahmen die unberechtigte Personen daran hindern, physischen Zutritt zum Betriebsgelände, den Gebäuden oder Räumen zu erhalten, in denen Systeme stehen, die personenbezogene Daten verarbeiten; Personen sind unberechtigt, wenn ihre Tätigkeit nicht mit den Aufgaben übereinstimmt, die ihnen zugewiesen wurden. Ausnahmen können für Auditoren von Dritten für die Zwecke der Prüfung der Einrichtungen gestattet werden, solange sie vom Auftragsverarbeiter überwacht werden und keinen Zugang zu den personenbezogenen Daten selbst erhalten. Insbesondere hat der Auftragsverarbeiter: 1. die Festlegung befugter Personen, einschließlich des Umfangs der Befugnisse 2. die Umsetzung einer Schlüsselregelung 3. die Umsetzung einer Besucherregelung (Abholung am Empfang und Begleitung durch Mitarbeiter) 4. das Vorhandensein und die regelmäßige Überprüfung von physischen Schutzmaßnahmen: ○ Gesicherter Eingang ○ Sicherheitstüren/-fenster sicherzustellen.

(2) Schutzmaßnahmen der **Zugangskontrolle:**
Maßnahmen die davor schützen, dass Unbefugte Zugang zu den Datenverarbeitungssystemen bekommen. Insbesondere hat der Auftragsverarbeiter: 1. sichergestellt, dass alle Computer (inkl. Remote-Rechner), die personenbezogene Daten verarbeiten, nach dem Neustart und bereits kurze Zeit nach dem Verlassen passwortgeschützt sind, um andere daran zu hindern, unberechtigten Zugriff auf personenbezogene Daten zu erhalten. 2. dedizierte User Ids für jede einzelne Person zur Authentifizierung an Benutzerverwaltungen der Systeme eingeführt, die zentral verwaltet werden (Single Sign On)

3. eindeutige Nutzerkonten und somit Passwörter für die Authentifizierung zugewiesen
4. sichergestellt, dass die Zugriffskontrolle über ein Berechtigungssystem erfolgt.
5. nur eigenem Personal oder Vorständen, Managern, Mitarbeitern, Vertretern und genehmigten Unterauftragsverarbeitern seiner genehmigten Unterauftragsverarbeiter Zugriff gestattet und ihnen nur die Berechtigungen auf personenbezogene Daten verarbeitende Anwendungen erteilt, die sie zur Ausführung ihrer Funktionen benötigen
6. sichergestellt, dass alle Wartungszugänge nur mit 2-Faktor-Authentifizierung zugänglich sind.
7. Eine Passwort-Policy implementiert, die das Teilen von Passwörtern verbietet, einen Prozess nach Bekanntgabe eines Passwortes beschreibt und das regelmäßige Ändern eines Passwortes verlangt
8. Sichergestellt, dass jeder Rechner eine passwortgeschützte Bildschirmsperre hat, welche spätestens 5 Minuten nach Inaktivität aktiviert wird.
9. Sichergestellt, dass Passwörter immer verschlüsselt oder gehashed gespeichert werden
10. Ein geeignetes Verfahren eingeführt, um Benutzerprofile zu deaktivieren, wenn der Benutzer das Unternehmen oder die Funktion verlässt
11. Einen geeigneten Prozess eingeführt, um die Administrator-Rechte anzupassen, wenn der Administrator das Unternehmen verlässt.

(3) Schutzmaßnahmen der **Zugriffskontrolle:**

Personen, die berechtigt sind, ein datenverarbeitendes System zu nutzen, sollen Zugriff nur auf die Daten erhalten, zu deren Zugriff sie berechtigt sind, und die personenbezogenen Daten dürfen im Rahmen der Verarbeitung nicht unberechtigt gelesen, kopiert, verändert oder gelöscht werden.

Insbesondere hat der Auftragsverarbeiter:

1. Zugriff auf Dateien und Daten basierend auf dem „Need-to-Know-Prinzip“ eingeschränkt
2. Datenträger mit personenbezogenen Daten in gesicherten Bereichen gelagert
3. die Installation von unberechtigter Hard- und Software verboten
4. Regeln für die sichere und dauerhafte Zerstörung von Daten aufgestellt, die nicht mehr benötigt werden
5. Nur eigenem Personal oder Vorständen, Managern, Mitarbeitern, Vertretern und genehmigten Unterauftragsverarbeitern seiner genehmigten Unterauftragsverarbeiter Zugriff gestattet und ihnen minimale Berechtigungen auf personenbezogene Daten erteilt, die sie zur Ausführung ihrer Funktionen benötigen
6. Personenbezogene Daten nicht grundlos vom Geschäftscomputer oder Gelände des Auftragsverarbeiters entfernen.

(4) Schutzmaßnahmen der **Trennungskontrolle:**

Die interne Organisation des Auftragsverarbeiters soll den speziellen Anforderungen des Datenschutzes entsprechen. Insbesondere separiert der Auftragsverarbeiter Daten, die nicht der blink.it GmbH & Co. KG gehören von denen, die der blink.it GmbH & Co. KG gehören durch technische und organisatorische Maßnahmen, um das versehentliche Mischen von personenbezogenen Daten zu vermeiden.

Insbesondere hat der Auftragsverarbeiter folgendes sichergestellt:

1. Trennung von Produktiv- und Testsystem
2. Limitierung des Datenbankzugriffs auf Personen und Prozesse die diese Daten zu Ausführung ihrer Tätigkeit benötigen.
3. Logische Mandantentrennung
4. Einholen der Verpflichtung der Mitarbeiter auf Einhaltung der Vertraulichkeit
5. Das Personal ist hinsichtlich Datenschutz und Datensicherheit geschult
6. Personenbezogene Daten verschiedener Kunden so hinterlegt, dass es in jedem Verarbeitungsschritt der für die Verarbeitung der personenbezogenen Daten verantwortliche identifiziert werden kann

(5) Schutzmaßnahmen der **Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO):**

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Information gesondert aufbewahrt werden und entsprechenden technische und organisatorischen Maßnahmen unterliegen.

Insbesondere stellt der Auftragsverarbeiter sicher:

1. Nutzeraktivitäten werden zu Zwecken der Abrechnung und Systemüberwachung in Datenbanken zur statistischen Analyse sowie einem Log-Service gespeichert. Die hier gespeicherten Daten sind pseudonymisiert. Die Daten sind für Dritte nicht mehr auf einen Nutzer zurückzuführen.

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

(6) Schutzmaßnahmen der **Weitergabekontrolle:**

Abgesehen von der für die Erbringung der in dieser Vereinbarung beschriebenen Dienstleistungen notwendigen Verarbeitung personenbezogener Daten dürfen diese nicht unberechtigt während der Übermittlung oder bei der Speicherung gelesen, kopiert, verändert oder gelöscht werden und es soll möglich sein herauszufinden, zu wem die personenbezogenen Daten übermittelt wurden.

Insbesondere wird der Auftragsverarbeiter:

1. Daten während jeglicher Übermittlung verschlüsseln (RSA 2048 bit Key mit einer SHA256 Signatur)
2. Übermittlungsprotokolle anfertigen

(7) Schutzmaßnahmen der **Eingabekontrolle:**

Es soll rückwirkend möglich sein festzustellen ob und durch wen personenbezogene Daten in das Datenverarbeitungssystem eingegeben, verändert oder gelöscht wurden.

Insbesondere wird der Auftragsverarbeiter:

1. Administrator- und Benutzeraktivitäten loggen
2. Nur berechtigtem Personal & Nutzern erlauben, personenbezogene Daten im Rahmen seiner Funktion zu ändern

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

(8) Schutzmaßnahmen der **Verfügbarkeitskontrolle:**
Personenbezogene Daten sollen gegen Weitergabe und versehentliche oder unberechtigte Zerstörung oder Verlust geschützt werden. Insbesondere wird der Auftragsverarbeiter: 1. Backup-Kopien erstellen 2. Regelmäßige Restore-Tests mit diesen Backups durchführen 3. Notfallpläne oder Strategien zur Wiederaufnahme des Geschäfts erstellen 4. Nicht privates Equipment zur Ausführung der Dienstleistungen nutzen 5. Sicherstellen, dass immer dann, wenn ein Benutzer seinen Schreibtisch unbeaufsichtigt verlässt und bevor er das Büro am Tagesende verlässt, er/sie sicherstellt, dass Dokumente, die personenbezogene Daten beinhalten, sicher aufbewahrt werden, wie beispielsweise in einer verschlossenen Schreibtischschublade, einem Aktenschrank oder einem anderen sicheren Lagerplatz. (clean desk) 6. Firewalls auf Netzwerkebene haben, um unberechtigten Zugriff auf Systeme und Services auf Netzwerkebene zu verhindern 7. Sicherstellen, dass auf jedem Computer-System eine geeignete Antivirus-Lösung läuft

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32.I. d) DSGVO; Art. 25.I DSGVO)

(9) Schutzmaßnahmen der **Auftragskontrolle:**
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Insbesondere wird der Auftragsverarbeiter: 1. Definierte Vergabekriterien für Subunternehmer (min. ISO-Zertifizierung 27001) 2. Auswahl des Auftragsverarbeiters unter Sorgfalts Gesichtspunkten (insbesondere hinsichtlich Datensicherheit) 3. Schriftliche Vereinbarungen mit allen Auftragsverarbeiter 4. Führen eines Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) 5. Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis 6. Regelmäßige Schulung der Mitarbeiter in Datenschutzangelegenheiten 7. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags 8. Überprüfung der Auftragsverarbeiter und ihrer Tätigkeiten 9. Regelmäßige Kontrollen und Überprüfung der internen Datenschutzvorkehrungen 10. Bestellung eines Datenschutzbeauftragten 11. Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

Anlage 2: Subunternehmer

Die vertraglich vereinbarten Leistungen/Teilleistungen werden unter Einschaltung von Subunternehmen durchgeführt, die in diese Verarbeitung mit einbezogen sind.Die Pflichten des Verantwortlichen aus dieser Vereinbarung sind vom Auftragsverarbeiter auch in Bezug auf die Subunternehmer sicherzustellen. Dies gilt insbesondere für gleichwertige Anforderungen an Vertraulichkeit, Gewährleistungen von Datenschutz und Datensicherheit, Kontrollrechte und die Informationspflicht bei Verstößen, Pflichtverletzungen und Produktionsstörungen, die möglicherweise eine Meldepflicht nach Art. 33 DSGVO oder eine Benachrichtigungspflicht nach Artikel 34 DSGVO (bei unrechtmäßiger Kenntniserlangung von Dritten) auslösen können. Nachstehend werden alle Subunternehmer aufgeführt, **die unmittelbar mit der Leistungserstellung für den Verantwortlichen beteiligt sind** und möglicherweise Zugriff auf die Daten des Verantwortlichen haben oder haben könnten. Dazu zählen auch externe IT-Dienstleister mit entsprechenden Zugriffsrechten. Nicht dazu gehören i.d.R. Telekommunikationsleistungen, Post-/Transportdienstleistungen.

Genehmigte Subunternehmer

Name	Amazon Web Services EMEA SARL
PLZ, Ort	L-1855 Luxembourg
Straße	38 Avenue John F. Kennedy
Land	Luxembourg
Aufgabe des Subunternehmers	Bereitstellung von Serverdiensten in den **Availability Zones Frankfurt am Main** (DIN 27001, BSI C5 zertifiziert). Alle Daten werden **nur** in Deutschland gespeichert und verarbeitet. Weitere Informationen zur Sicherheit/Compliance von Amazon AWS unter: https://aws.amazon.com/de/compliance/

Prüfung der TOMs durch:

Christopher Hutz dapex – data protection experts SH Beratung & Beteiligung UG (haftungsbeschränkt)	Datum: 19.04.2021	Unterschrift: