Vereinbarung zur Auftragsverarbeitung nach Art. 28 Datenschutzgrundverordnung (DSGVO)

Zwischen

[Verantwortlicher],

[Anschrift]

– nachfolgend „Auftraggeber bzw. Verantwortlicher" genannt –

und

adventics GmbH

Münchener Str. 23a

85540 Haar bei München

– nachfolgend als Anbieter und Betreiber des Systems Scan2lead und somit „Auftragnehmer bzw. Auftragsverarbeiter" genannt –

und gemeinsam als „Vertragsparteien" bezeichnet – wird Folgendes vereinbart:

1. Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

2. Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

3. Weisungsberechtigte des Auftraggebers, Weisungen an den Auftragnehmer

(1) Weisungsberechtigte Personen des Auftraggebers sind:

- _____

(2) Weisungsempfänger beim Auftragnehmer sind:

- Bernhard Gamper, Geschäftsführer, Tel. +49 (89) 4444 33 130, bernhard.gamper@adventics.de
- Gunnar Heinrich, Geschäftsführer, Tel. + 49 (89) 4444 33 140, gunnar.heinrich@adventics.de

(3) Für Weisung zu nutzende Kommunikationskanäle:

- Bevorzugt E-Mail

(4) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolgerbzw. die Vertreter mitzuteilen.

4. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die im Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die in Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

5. Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhalten-

en personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im Anhang 1 mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

6. Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

7. Einsatz von Subunternehmern als weitere Auftragsverarbeiter

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens drei Wochen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden mit der Unterrichtung über die geplante Beauftragung zur Verfügung. Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 7 Abs. 2 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

(2) Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten

Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Artikel 44 ff. DSGVO sicher, indem – sofern erforderlich - geeignete Garantien gemäß Artikel 46 DSGVO getroffen werden.

(4) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(5) Im Falle des Abschnitt 7 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

8. Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Kosten hierfür trägt der Verantwortliche. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(3) Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Prüfungen in angemessenem Umfang unterstützend mitwirkt. Anfallende Aufwände bis zu 4 Stunden werden vom Auftragsverarbeiter getragen. Alle

darüber hinaus anfallenden Aufwendungen werden von Verantwortlichen getragen.

(4) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

9. Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei insbesondere folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

10. Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

11. Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Für Vertragsbegründungen, Vertragsänderungen und Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronischesFormat erforderlich.

(3) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Auftraggeber und Auftragnehmer werden sich in diesem Fall sowie im Fall einer regelungsbedürftigen Lücke auf eine Lösung verständigen, die dem der wirtschaftlichen Zielsetzung aller Beteiligten (Auftraggeber, Auftragnehmer, Empfänger und betroffene Personen) am nächsten kommt.

Aussteller:

Anhang 1

Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Bereitstellung der Anwendung Scan2Lead: Betrieb, Wartung und Support der Anwendungssoftware Betrieb der Anwendung Scan2Lead: Erfassung und Zuordnung von Kontakt- und Adressdaten (Erfassung des Barcodes des Besucherausweises und Kontaktdaten der Besucher auf den Visitenkarten
Art und Zweck der Verarbeitung	Bereitstellung der Anwendung: Die Daten werden zur Erstellung und Verwaltung des Zugangs der Anwendung erhoben, gespeichert und verarbeitet. Betrieb der Anwendung: Analyse und Abgleich der Daten zur Sortierung und Bereitstellung von Kontakt- und Adressdaten für den Import in das CRM-System des Ausstellers.
Art der personenbezogenen Daten	Bereitstellung der Anwendung: - Name, - Vorname, - E-Mailadresse. Betrieb der Anwendung: - Anrede, - ggf. Titel, - Vorname, - Nachname, - Bild, - Unternehmen, - Funktion, - Telefonnummer, - Mobilfunknummer, - E-Mailadresse, - Anschrift, - ggf. USt-ID, - LinkedIn- / Xing- Profil.
Kategorien betroffener Personen	Bereitstellung der Anwendung: Mitarbeiter des Auftraggebers (Aussteller) Betrieb der Anwendung:

	Potentielle und bestehende Kunden sowie Geschäftspartner der Aussteller
Dauer der Verarbeitung	Die Auftragsdauer ergibt sich aus der Dauer des Auftrags bzw. der tatsächlichen Nutzung durch den Auftraggeber.

Datenschutzbeauftragte/r des Verantwortlichen	[...]
Datenschutzbeauftragte/r des Auftragsverarbeiters	datenschutz süd GmbH Wörthstraße 15 97082 Würzburg Tel.: +49 931 30 49 76 0

Anhang 2

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

SUBUNTERNEHMER	STANDORT DER VERARBEITUNG	ART DER VERARBEITUNG	MIT DEM SUBUNTERNHEMER VEREINBARTE GARANTIEN*
Microsoft Ireland Operations Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D 18 P 521, Irland	MS Azure Cloud Services zur Datenverwaltung und Speicherung	EU-Standradvertragsklauseln, Angemessenheitsbeschluss (EU-U.S. Data Privacy Framework)
ABBYY Europe GmbH	Friedenstraße 22B, 81671 München, Deutschland	Modul zur Visitenkartenerkennung	
ActiveCampaign LLC („Postmark“)	1 N Dearborn St FL5, Chicago, IL 60602, USA	E-Mail-Versand (Info-E-Mails an Scan2Lead-Nutzer)	EU-Standradvertragsklauseln, Angemessenheitsbeschluss (EU-U.S. Data Privacy Framework)
Zoho Corporation Pvt. Ltd.	Beneluxlaan 4B, 3527 HT Utrecht, Niederlande	E-Mail-Versand, interne Verwaltung, Verwaltung von Kundendaten und Kundensupport, Abrechnungen	

*Garantien können u.a. EU-Standardvertragsklausel (SCC), genehmigte Binding Corporate Rules (BCR) oder auch ein Angemessenheitsbeschluss sein.

Anhang 3

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

Gesellschaft / Standort

Die nachstehenden technischen und organisatorischen Sicherheitsmaßnahmen beziehen sich auf:

- **adventics GmbH**

  Münchener Str. 23A

  85540 Haar bei München, Deutschland
- **adventics GmbH**

  Seidlgasse 34

  1030 Wien, Österreich

A. Art. 32 DSGVO

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 trifft die adventics GmbH geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

B. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

B.1. Zutrittskontrolle

Definition

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

B.1.1. Bürogebäude

- Die Büroräume der adventics GmbH in Deutschland befinden sich in der Münchner Str.23A, 85540 Haar bei München.
- Die Büroräume der adventics GmbH in Österreich befinden sich in der Seidlgasse 34, 1030 Wien.
- Die Büroräume sind mit einem mechanischen Schließsystem versehen.
- Die Schlüsselausgabe an Mitarbeitern wird protokolliert.
- Die Schlüsselvergabe findet durch die Geschäftsleitung statt.

B.1.2. Besucherregelungen

- Per Zutrittsregelung dürfen sich Besucher nur in ständiger Begleitung mit dem zuständigen Ansprechpartner in den Büroräumlichkeiten bewegen.

B.1.3. Zutritt Serverraum

- Die Serverräume der adventics, auf denen personenbezogenen Daten verarbeitet werden, befinden sich in Europa. Die Server werden gehostet durch:

- Microsoft Azure EU Data Center Europe West/ Niederlande

  Das Azure Data Center Europe West hat folgende Zertifizierungen: CIS Benchmark | CSA-STAR attestation | CSA-STAR certification | CSA-STAR self-assessment ISO 20000-1:2011 | ISO 22301 | ISO 27001 | ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001 PCI DSS | SOC | WCAG | CDSA | PCI DSS | Shared Assessments | TruSight | BIR 2012 | AFM + DNB NEN-7510

  https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure
- Zoho EU Data Center Amsterdam, Niederlande

  Das Zoho Data Center in den Niederlanden hat folgende Zertifizierungen: ISO 27001 ISO 22301 SOC 2 TYPE IIISO 50001 PCI DSS

B.2. Zugangs- und Zugriffskontrollmaßnahmen

Definition

Maßnahmen, die sicherstellen, dass

- Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können,
- der Versuch des unbefugten Zugangs nicht unbemerkt bleibt,
- die zur Benutzung der Datenverarbeitungsanlagen befugten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und unbefugtes Lesen, Kopieren, Ändern verhindert wird,
- der Versuch des unbefugten Zugriffs nicht unbemerkt bleibt.

B.2.1. Zugangsberechtigungen

- Definierter Freigabeprozess, welcher Mitarbeiter auf welche personenbezogene Daten Zugang hat.
- Vergabe bzw. Zugriffsberechtigungen werden protokolliert.
- Jeder Mitarbeiter erhält ein personalisiertes Benutzerkonto.
- Jeder Mitarbeiter muss sich bei jeden Log-In über einer 2-Faktor-Authentifizierung identifizieren.
- Es existiert ein Passwort-Parameter:
  - Das Passwort enthält mindestens 8 Zeichen,
  - Passwörter beinhalten jeweils Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen,
  - Passwörter dürfen nicht leicht zu erraten sein (Geburtsdatum),
  - Trivialpasswörter (1111) dürfen nicht verwendet werden,
  - Bereits genutzte Passwörter dürfen nicht erneut verwendet werden.
- Das System zwingt zur Einhaltung der Passwortvorgabe.
- Bei Inaktivität schaltet sich der Bildschirm nach 5 Minuten ab.
- Sollte der Verdacht auf Kompromittierung bestehen, muss das Passwort unmittelbar durch die 2-Faktor- Authentifizierung geändert werden.
- Die Anmeldeversuche sind begrenzt und bleiben bis zur manuellen Aufhebung durch die IT auch gesperrt.
- Bei Fernzugängen erfolgt die Identifizierung der Mitarbeiter ebenfalls über eine 2-Faktor-Authentifizierung.

- Die Anmeldeversuche bei Fernzugriffen sind begrenzt und bleiben bis zur manuellen Aufhebung durch die IT auch gesperrt.

B.3. Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten

Definition

Maßnahmen, die die Umsetzung von geeigneten technischen und organisatorischen Maßnahmen auch auf mobilen Datenträgern und Endgeräte sowie auf Papier-Unterlagen gewährleisten.

B.3.1. Papierunterlagen

- Vertrauliche und geheime Informationen in Papierform sind ausschließlich über den im Unternehmen zur Verfügung gestellten Schreddern (Sicherheitsstufe P4) zu entsorgen.

B.3.2. Mobile Datenträger und mobile Endgeräte

- Es werden Datenträger für den Austausch von Daten genutzt. Datenträger von unbekannter Herkunft dürfen nicht zusammen mit Firmenhardware verwendet werden.
- Die zum Datenaustausch genutzten mobilen Datenträger, wie z. B. USB-Sticks sind auf der Festplatte zu verschlüsseln.
- Der Gebrauch von privaten mobilen Endgeräten ist untersagt.
- Die Entsorgung von mobilen Endgeräten und Datenträgern erfolgt durch die IT-Abteilung.

B.3.3. Maßnahmen zur sicheren Datenübertragung

Definition

Maßnahmen, die sicherstellen, dass

- Daten bei der elektronischen Übertragung oder während des Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Ein Transport von physischen Datenträgern mit personenbezogenen Daten zu einem Aktenvernichtungsdienstleiter nur in geschlossenen Behältnissen und in geschlossenen Fahrzeugen durchgeführt wird, so dass keine Daten verloren gehen können.

B.3.4. Weitergabekontrolle

- E-Mails werden per TLS übermittelt.
- Betrieb und Einsatz eines FTP-Servers, über den das File-Sharing und der sichere bzw. verschlüsselte Versand von Dateien gewährleistet ist.
- Datenträger, die für den Austausch von Daten genutzt werden, sind verschlüsselt.
- Die Schlüssel bzw. Zertifikate werden durch die hauseigene IT verwaltet.

C. Maßnahmen zur Sicherstellung der Verfügbarkeit

Definition

Maßnahmen zur Datensicherung (physikalisch / logisch) gegen zufällige Zerstörung oder Verlust.

C.1. Serverraum

- Bei den Serverraum handelt es sich um einen innenliegenden Raum ohne Fenster.
- Der Serverraum ist mit einer feuerhemmenden Zugangstür aus Massivwand geschützt.
- Der Serverraum ist an die Brandmeldezentrale angeschlossen.
- Der Serverraum ist sowohl mit einem Löschsystem (CO2 Löscher und Halon/ Argon Löschanlage) als auch mit einer Klimatisierung ausgestattet.
- Unterbrechungsfreie Stromversorgung, welche zusätzlich durch ein Dieselaggregat abgesichert und deren Funktionalität regelmäßig getestet wird.

C.2. Backup- und Notfall-Konzept, Virenschutz

- Dokumentiertes Backup-Konzept.
- Regelmäßiges Testen des Backup-Konzeptes.
- Die Durchführung und Dokumentation des Backup Checks findet in regelmäßigen Abständen aber mindestens zweimal im Monat statt.
- Die Durchführung und Dokumentation der Backup Checks werden durch die externen Dienstleister Microsoft Azure und Zoho durchgeführt.
- Die regelmäßige Erstellung von Backups erfolgt auf dem Online Cloud Speicher der genannten externen Dienstleister.
- Die Lagerung der Backups erfolgt in einem vom primären Server getrennten Abschnitt.

C.2.1.1. Change- und Patchmanagement

- Dokumentation des Change- und Patchmanagements, welches durch die hauseigene IT zu verantworten ist.

C.2.1.2. Notfallvorsorgekonzept

- Dokumentation eines Notfallvorsorgekonzeptes mit genauen Handlungsvorgaben.

C.3. Virenschutz

- Alle Server und Clients sind mit einem Virenschutz versehen, welcher stetig von der hauseigenen IT aktualisiert wird. Es dürfen grundsätzlich keine Rechner ohne aktuellen Virenschutz betrieben werden.

C.4. Netzanbindung

- Die gesamte Netzanbindung wird von der hauseigenen IT betrieben und ist bezüglich der einzelnen Standorte nicht redundant miteinander verbunden.

D. Pseudonymisierung/Verschlüsselung, Art. 32 Abs. 1 lit. a DSGVO

Definition

Die Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DSGVO) gewährleistet, dass Identifikationsmerkmale personenbezogener Daten, sofern dies zum Schutz der betroffenen Personen erforderlich ist oder aus datenschutzrechtlicher Sicht geboten ist, bestimmter oder bestimmbarer Personen durch Kennzeichen ersetzt werden und daher die Zuordnung zur betroffenen Person nicht ohne zusätzliche Informationen möglich ist. Folglich können Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person

zugeordnet werden. Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

D.1. Einsatz von Pseudonymisierung

- Sofern möglich, werden Daten pseudonym verarbeitet.
- Soweit Daten im Rahmen der beauftragten Verarbeitung analysiert werden, findet eine datenschutzgerechte Pseudonymisierung oderAnonymisierung statt. Weiterhin ist eine Pseudonymisierung von Daten im Gesamtprozess insofern gewährleistet,dass auf scanbaren Zutrittsausweisen der Besucher und Aussteller („Badges") lediglich eine eindeutige, i.d.R. nicht fortlaufende Nummer aufgedruckt bzw. im 1D oder 2D Barcode codiert, die erst im Rahmen der verschlüsselten Kommunikation der Scan2Lead Frontend- Geräte mit den Backend-Systemen mit den Personendaten des jeweiligen Besuchers zusammengeführt wird.
- Die Zuordnung und Speicherung von einzelnen Daten erfolgen in getrennt Systemen voneinander.

D.2. Einsatz von Verschlüsselung

- Sofern möglich, sind Daten verschlüsselt zu verarbeiten. Dies ist Einzelfall- und projektabhängig zu beurteilen.
- Die Kommunikation zwischen den Frontend-Geräten der Scan2Lead Anwender und den Backend-Systemen findet ausschließlich unter Einsatz gängiger Verschlüsselungsverfahrenstatt.

E. Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen - Art. 32 Abs. 1 lit. b, c, d DSGVO

E.1. Durchführung von Systemaudits

- Systemaudits zur Überprüfung der bestehenden Systeme und ob diese funktionieren.
- Sollten sich Abweichungen bzw. Nicht-Konformitäten ergeben, werden diese in der Risikobewertung aufgenommen und entsprechende Gegenmaßnahmen eingeleitet.
- Stetige Überprüfung und Dokumentation der Ergebnisse.

E.1.1. Datenschutzmanagement

- Bestellung eines betrieblichen Datenschutzbeauftragten
- Verpflichtung zur Einhaltung des Datenschutzes nach Maßgabe der DSGVO
- Information der Beschäftigten zu den Themen Datenschutz und Datensicherheit durch Schulungen und schriftlichen Erläuterungen (Anhang zur Verpflichtungserklärung)
- Durchführung von Präsenzschulungen sowie E-Learnings (z.B. bei Einstellung) zu datenschutzrechtlichen Themen
- Abschluss von Verträgen zur Auftragsverarbeitung gemäß Art. 28 DSGVO
- Weitergabe der Verpflichtungen aus dem schriftlichen Vertrag zur Auftragsverarbeitung an Unterauftragnehmer
- Richtlinien und Checklisten zur Beauftragung von Dienstleistern
- Kontrolle der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen
- Information des Auftraggebers bei Fehlern/ Unregelmäßigkeiten in der Datenverarbeitung

- Erläuterungen und Richtlinien zu datenschutzrechtlichen Themen und Vorgaben aus der DSGVO (z.B. Umgang mit Betroffenenanfragen / Vorgehen im Falle einer „Datenpanne“ etc.).

E.1.2. Dokumentation

- Die getroffenen Maßnahmen werden kontinuierlich überprüft und bei Erforderlichkeit überarbeitet.