Allgemeine Geschäftsbedingungen (AGB)

SOC-Vertrag ("Security Operations Center“)

Inhaltsverzeichnis

Teil 1 Allgemeine Angaben

1. Allgemeine Bestimmungen

1.1 Diese Allgemeinen Geschäftsbedingungen ("AGB") regeln die Vertragsbeziehungen zwischen der DigiFors GmbH („DigiFors“), Torgauer Straße 231, 04347 Leipzig und ihrem Vertragspartner ("Kunde"), sofern beide Parteien Unternehmer im Sinne von § 14 BGB sind.

1.2 Diese AGB gelten für die Bereitstellung für die Dienstleistungen im Rahmen eines SOC-Vertrags ("Security Operations Center"), der insbesondere das IT-Security-Monitoring umfasst.

1.3 Abweichende, entgegenstehende oder ergänzende Bedingungen des Kunden finden keine Anwendung, es sei denn, DigiFors hat ihrer Geltung ausdrücklich schriftlich zugestimmt.

2. Vertragsgegenstand, Vertragsbeginn

2.1 Gegenstand dieses Vertrags ist die Bereitstellung eines Security Operations Centers (SOC) durch DigiFors.

Die vertraglich geschuldete Leistung umfasst ein IT-Security Monitoring der gesamten IT-Infrastruktur des Kunden („Dienstleistung“). Die IT-Infrastruktur ergibt sich aus den vom Kunden bereitgestellten Angaben und umfasst ausschließlich die IT-Systeme und Komponenten, die der Kunde DigiFors ausdrücklich benannt und zur Überwachung freigegeben hat.

Zur Erbringung der Dienstleistung werden Daten der Infrastrukturkomponenten an einer zentralen Stelle gesammelt. Die Erhebung dieser Daten erfolgt entweder durch die Installation einer Client-Software auf den Endgeräten oder durch die Übermittlung von Logfiles. Hierfür wird die Open-Source-Sicherheitsplattform Wazuh eingesetzt.
Darüber hinaus werden zur Leistungserbringung durch das SOC weitere Komponenten für Alarmierung und Ticketing betrieben. Die DigiFors ist in der Auswahl der entsprechenden Werkzeuge frei, sofern diese den geltenden Datenschutzbestimmungen sowie den anerkannten Regeln der Technik entsprechen.
Jegliche Überwachung oder Verarbeitung von Daten erfolgt ausschließlich im Rahmen der vertraglichen Vereinbarungen und unter Beachtung der geltenden gesetzlichen Bestimmungen, insbesondere des Datenschutzrechts.

2.2 Der Vertrag gliedert sich in zwei Phasen:

a. Installations- und Einschwingphase: Die Einschwingphase dauert maximal 2 Monate. Nicht beendete Arbeiten, wie z.B. das Anbinden von weiteren Datenquellen, erfolgen dann im Regelbetrieb.

b. Überwachungsphase („Regelbetrieb“): Im Folgemonat der Beendigung der Einschwingphase beginnt die dauerhafte IT-Sicherheitsüberwachung durch DigiFors. Arbeiten, die am Ende der Einschwingphase nicht oder nur teilweise fertiggestellt sind, werden in den Regelbetrieb übernommen und über das in der monatlichen Pauschale hinterlegte Jahresstundenkontingent abgebildet. Das gilt auch für die weitere Anbindung von Datenquellen.

2.3 Der Vertrag beginnt mit dem Start der Installations- und Einschwingphase von maximal 2 Monaten. Die vereinbarte Laufzeit der Überwachungsphase („Regelbetrieb“) beginnt in dem Folgemonat der Installations- und Einschwingphase und beträgt nach Wahl des Kunden und getroffener Vereinbarung 12, 24 oder 36 Monate.

3. Vertragsschluss

3.1 Der Vertrag kommt durch Annahme eines Angebots von DigiFors durch den Kunden zustande. Die Präsentation unserer Dienstleistung stellt kein bindendes Angebot dar. Erst die Beauftragung der Dienstleistung durch den Kunden ist eine bindende Annahme des Angebot nach § 145 BGB. Die Einschwingphase beginnt zum vereinbarten Termin.

3.2 Nach Abschluss der Einschwingphase beginnt automatisch die Überwachungsphase mit der jeweils vereinbarten Vertragslaufzeit.

4. Leistungsumfang

4.1 Die in den schriftlichen Angebotsunterlagen ggf. enthaltene Leistungsbeschreibung, die dem Kunden vor seiner Auftragserteilung überlassen oder in gleicher Weise wie diese AGB in den Vertrag einbezogen wurde (im Folgenden auch „Leistungsbeschreibung“), ist alleinige Grundlage für die von DigiFors zu erbringenden Leistungen. Enthalten die schriftlichen Angebotsunterlagen keine Leistungsbeschreibung, ergibt sich der Leistungsumfang aus dem Angebotsinhalt.

4.2 Im Rahmen des Regelbetriebes wird DigiFors auf sicherheitsrelevante Vorfälle oder Verdachtsfälle in drei Prioritätsstufen reagieren, Näheres dazu ergibt sich aus der Leistungsbeschreibung.

DigiFors verpflichtet sich, alle Vorfälle gemäß den Prioritäten zu kategorisieren und eine entsprechende Reaktionszeit sicherzustellen. Bei außergewöhnlichen Umständen kann die Reaktionszeit angepasst werden, über die der Kunde unverzüglich informiert wird.

4.3 Technische oder sonstige Normen sind nur dann einzuhalten, soweit sie in der

Leistungsbeschreibung ausdrücklich aufgeführt sind, und zwar in der bei Vertragsschluss geltenden Fassung.

4.4 Soweit Softwareprodukte installiert und/oder zur Nutzung überlassen werden, die nicht von DigiFors entwickelt wurden, gelten vorrangig die Lizenzbedingungen des jeweiligen Herstellers bzw. Lizenzgebers. Soweit es sich um Open-Source-Software handelt, gelten hierfür vorrangig die entsprechenden Open-Source-Lizenzbedingungen, jedoch nur soweit diese den vertraglichen Nutzungsumfang und die Mängelhaftung nicht einschränken.

4.5 DigiFors ist berechtigt, Dritte als Subunternehmer und Erfüllungsgehilfen bei der Leistungserbringung einzusetzen.

5. Preise und Zahlungsbedingungen

5.1 Sofern im Einzelfall nicht anderes vereinbart ist, gelten als vertraglich vereinbarte Preise die in den DigiFors Angebotsunterlagen genannten Nettopreise, jeweils zzgl. gesetzlicher Umsatzsteuer und Abgaben.

5.2 Die Kosten für die Installations- und Einschwingphase fallen bereits während dieser Phase an und sind gesondert zu begleichen. Der Zahlungsplan ergibt sich aus dem Angebot.

5.3 DigiFors ist berechtigt, die vertraglich vereinbarte Vergütung mit einer schriftlichen Ankündigung von 3 Monaten zum Änderungszeitpunkt zu ändern. Eine Änderung darf grundsätzlich frühestens 24 Monate nach Vertragsschluss oder nach der letzten Vergütungserhöhung erfolgen. Die Änderung erfolgt unter Einhaltung der folgenden Grundsätze:

- DigiFors darf die Vergütung höchstens in dem Umfang ändern, in dem sich der nachfolgend genannte Index seit Vertragsbeginn (mindestens um 3 % nach oben oder unten) verändert hat.
- Für die Ermittlung des Änderungsrahmens ist der Erzeugerpreisindex für IT-Dienstleistungen des Statistischen Bundesamts zugrunde zu legen.
- Bei dieser Änderung sind auch etwaige Kostenminderungen zu berücksichtigen und anzurechnen.

DigiFors hat die Höhe der Anpassung dem Kunden in Textform mitzuteilen. Wenn sich der Kunde nicht binnen 4 Wochen ab Zugang der Anpassungserklärung hierzu erklärt, gilt die neue Vergütung als vereinbart. DigiFors wird den Kunden im Rahmen der schriftlichen Ankündigung der Vergütungsanpassung insbesondere auf die Folgen einer ausgebliebenen Erklärung und die darauf bezogene Frist hinweisen

5.4 Die Vergütung ist fällig und zu zahlen innerhalb von 14 Tagen nach Rechnungsdatum. Bei Zahlung per SEPA-Lastschrift Mandat wird der Rechnungsbetrag 14 Tage nach Rechnungsstellung abgebucht.

5.5 Mit Ablauf der Zahlungsfrist gemäß vorstehender Ziffer 5.4 kommt der Kunde in Verzug. Die Vergütung ist während des Verzuges zum jeweils geltenden gesetzlichen Verzugszinssatz zu verzinsen. DigiFors behält sich die Geltendmachung eines weitergehenden Verzugsschadens vor. Gegenüber Kaufleuten bleibt der Anspruch auf den kaufmännischen Fälligkeitszins (§ 353 HGB) unberührt.

5.6 Der Kunde kann nur mit solchen Forderungen aufrechnen, die unbestritten oder rechtskräftig festgestellt sind. Diese Einschränkung des Aufrechnungsrechts gilt nicht, wenn die zur Aufrechnung gestellte Geldforderung aus einem Anspruch erwächst, dessentwegen der Kunde auch zurückbehalten könnte oder hätte zurückbehalten können.

5.7 Wird nach Abschluss des Vertrags erkennbar, dass der Anspruch auf die vereinbarte Vergütung von DigiFors durch mangelnde Leistungsfähigkeit des Kunden gefährdet wird (z.B. durch Antrag auf Eröffnung des Insolvenzverfahrens), so ist DigiFors nach den gesetzlichen Vorschriften zur Leistungsverweigerung und – ggf. nach Fristsetzung – zum Rücktritt vom Vertrag berechtigt (§ 321 BGB).

5.8 Im Falle einer schuldhaften Pflichtverletzung durch den Kunden, insbesondere bei Nichterfüllung, Verzug oder unberechtigtem Rücktritt vom Vertrag, ist DigiFors berechtigt, einen pauschalen Schadensersatz in Höhe von 25% des vereinbarten Netto-Auftragswertes zu verlangen. Der Nachweis darüber, dass gar kein Schaden oder ein geringerer Schaden entstanden ist, bleibt dem Kunden ausdrücklich vorbehalten. Ebenso bleibt DigiFors das Recht vorbehalten, einen nachweislich höheren Schaden geltend zu machen, wobei die pauschalierte Summe in diesem Fall auf den Gesamtschaden angerechnet wird. Diese Pauschalierung gilt nicht bei Vorsatz oder grober Fahrlässigkeit sowie bei gesetzlichen Ansprüchen, insbesondere aus Produkthaftung oder wegen Verletzung von Leben, Körper oder Gesundheit.

6. Mitwirkungspflichten des Kunden

6.1 Der Kunde verpflichtet sich, DigiFors alle erforderlichen Informationen und Zugänge zu seiner IT-Infrastruktur bereitzustellen, um die ordnungsgemäße Installation und Überwachung zu ermöglichen.

6.2 Der Kunde hat sicherzustellen, dass die IT-Geräte, auf denen die Software installiert wird, die technischen Mindestanforderungen erfüllen.

6.3 Der Kunde ist verpflichtet, alle notwendigen Mitwirkungshandlungen vorzunehmen, insbesondere:

- Bereitstellung von Zugangsdaten und Zugängen
- rechtzeitige Information über Änderungen in der IT-Infrastruktur
- Sicherstellung, dass die Software (Agenten) gemäß den Anweisungen von DigiFors installiert und betrieben wird
- Sicherstellung, dass die Logdaten-Quellen gemäß den Anweisungen von DigiFors konfiguriert und betrieben werden
- Einstufung von Systemen nach Kritikalität bzw. Wichtigkeit
  Unterlässt der Kunde notwendige Mitwirkungshandlungen, haftet er für daraus entstehende Verzögerungen, Mehrkosten oder Schäden.

6.4 Der Kunde ist verantwortlich für die Einhaltung aller gesetzlichen Vorgaben im Zusammenhang mit der Nutzung der Software und der Dienstleistungen, insbesondere im Bereich Datenschutz.

7. Datenschutz, Auftragsverarbeiter

7.1 Soweit DigiFors auf personenbezogene Daten des Kunden oder aus dessen Bereich zugreifen kann, wird DigiFors ausschließlich als Auftragsverarbeiter im Sinne des Art. 4 Ziffer 8 in Verbindung mit Art. 28 DSGVO tätig und diese Daten nur zur Vertragsdurchführung verarbeiten und nutzen. DigiFors wird Weisungen des Kunden für den Umgang mit diesen Daten beachten. Der Kunde trägt etwaige nachteilige Folgen solcher Weisungen für die Vertragsdurchführung. Der Kunde wird mit DigiFors die Details für den Umgang mit den Daten des Kunden nach den datenschutzrechtlichen Anforderungen vereinbaren.

7.2 Der Kunde bleibt sowohl allgemein im Auftragsverhältnis als auch im datenschutzrechtlichen Sinne der Verantwortliche. Für das Verhältnis zwischen DigiFors und Kunde gilt: Gegenüber den Betroffenen trägt die Verantwortung für die Verarbeitung personenbezogener Daten der Kunde, außer soweit DigiFors etwaige Ansprüche der betroffenen Person wegen einer zuzurechnenden Pflichtverletzung zu vertreten hat. Der Kunde wird etwaige Anfragen, Anträge und Ansprüche der betroffenen Person verantwortlich prüfen, bearbeiten und beantworten. Das gilt auch bei einer Inanspruchnahme von DigiFors durch eine betroffene Person. DigiFors wird den Kunden dabei im Rahmen seiner Pflichten unterstützen, **siehe Teil 3 Vereinbarung zur Auftragsverarbeitung.**

7.3 DigiFors gewährleistet, dass Daten des Kunden ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeitet werden, soweit nichts anderes vereinbart ist.

8. Haftung

8.1 DigiFors haftet für Schäden, gleich aus welchem Rechtsgrund, nur bei Vorsatz und grober Fahrlässigkeit.

8.2 Bei leichter Fahrlässigkeit haftet DigiFors nur bei Verletzung einer wesentlichen Vertragspflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf (Kardinalpflicht). In diesem Fall ist die Haftung von DigiFors auf den vorhersehbaren, typischerweise eintretenden Schaden, maximal jedoch bis zu einem Betrag von fünf Millionen Euro begrenzt.

8.3 DigiFors haftet nicht für Schäden, die durch die Software eines Dritten verursacht werden. DigiFors übernimmt keine Haftung für Probleme, die durch Inkompatibilitäten zwischen Drittsoftware und der IT-Infrastruktur des Kunden oder durch Fehler in Updates der Drittsoftware entstehen.

8.4 Die Haftungsbeschränkungen gelten nicht bei Verletzung von Leben, Körper oder Gesundheit sowie bei Ansprüchen nach dem Produkthaftungsgesetz.

8.5 Die Verpflichtung des Kunden zur Schadensabwendung und Minderung, insbesondere im Fall von Daten- oder Dateiverlusten bleibt unberührt. Der Verlust von Daten ist nicht ersatzfähig, soweit für diese nicht regelmäßig – mindestens einmal täglich – Sicherungskopien auf getrennten Datenträgern erstellt wurden.

9. Laufzeit und Kündigung

9.1 Der Vertrag hat eine Mindestlaufzeit von 12, 24 oder 36 Monaten, je nach Vereinbarung zusätzlich zu der vorherigen Einschwingphase, welche maximal 2 Monate beträgt.

9.2 Eine ordentliche Kündigung ist während der Mindestlaufzeit ausgeschlossen. Der Vertrag verlängert sich automatisch um 12 Monate, sofern er nicht mit einer Frist von drei Monaten zum Ende der Laufzeit gekündigt wird.

9.3 Das Recht zur außerordentlichen Kündigung bleibt unberührt.

9.4 Die Kündigung des Vertrags bedarf der Schriftform.

10. Verjährung

10.1 Die wechselseitigen Ansprüche der Vertragsparteien verjähren nach den gesetzlichen Vorschriften, soweit nachfolgend nichts anderes bestimmt ist.

10.2 Die Verjährungsfrist für Gewährleistungsansprüche aus Sach- und Rechtsmängeln für Waren beträgt ein Jahr ab Ablieferung bzw. Überlassung. Die Verkürzung der Verjährungsfrist gilt nicht bei Vorsatz seitens DigiFors, arglistigem Verschweigen des Mangels und Personenschäden.

11. Gerichtsstand und anwendbares Recht

11.1 Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

11.2 Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Leipzig, sofern nicht ein anderer Gerichtsstand gesetzlich zwingend angeordnet ist. DigiFors ist auch berechtigt, am Hauptsitz des Kunden zu klagen.

12. Streitbeilegungsverfahren

12.1 Die Parteien verpflichten sich, im Falle von Streitigkeiten zunächst ein Mediationsverfahren durchzuführen. Das Mediationsverfahren wird von einem unabhängigen Mediator durchgeführt, der von beiden Parteien einvernehmlich benannt wird.

12.2 Scheitert die Mediation, steht der Rechtsweg offen.

13. Schlussbestimmungen

13.1 Nebenabreden bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

13.2 Erfüllungsort für sämtliche Leistungen und Lieferungen ist Leipzig.

13.3 Sollten einzelne Bestimmungen dieser AGB unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen Bestimmung tritt eine wirksame Regelung, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Gleiches gilt für den Fall, dass die AGB lückenhaft sind.

Teil 2 Vertraulichkeitsvereinbarung

Mit Annahme des AGBs werden folgende Regelungen zum Schutz von Informationen vereinbart:

1. Die Parteien verpflichten sich, den - zu dem vorbezeichneten Zweck - entstehenden Kontakt, sämtliche Inhalte dieser Vertraulichkeitsvereinbarung sowie jede - im vorgenannten Rahmen erhaltene und als vertraulich gekennzeichnete oder bezeichnete - Information, wie beispielsweise Unterlagen, Spezifikationen, Entwürfe, Pläne, Zeichnungen, Softwarematerialien, Daten, Muster, Prototypen, unkörperliche Informationen, wie Geschäftsideen oder Konzepte, insbesondere in schriftlicher, mündlicher, visueller oder elektronischer Form als ihr anvertraute Geschäfts- und Betriebsgeheimnisse - nachstehend „vertrauliche(n) Informationen“ genannt - streng vertraulich zu behandeln und Dritten gegenüber geheim zu halten.

2. Die Parteien verpflichten sich, die erhaltenen vertraulichen Informationen nur zum vorgesehenen Zweck zu verwenden, die Informationen nicht selbst zu verwerten, insbesondere keine Schutzrechtsanmeldungen vorzunehmen. Die Parteien sind jedoch berechtigt, Konzernunternehmen (i.S.d. §§ 15 ff AktG verbundene Unternehmen) und/oder den von ihnen im Zusammenhang mit der Zusammenarbeit eingeschalteten, von Berufs wegen zur Verschwiegenheit verpflichteten Beratern die nach ihrem Ermessen erforderlichen vertrauliche Informationen zugänglich zu machen. Durch die - die vertraulichen Informationen entgegennehmende - Partei wird außerdem sichergestellt, dass sämtliche Mitarbeiter oder sonstige Berater, denen die vertraulichen Informationen zugänglich gemacht werden müssen, soweit dies noch nicht geschehen ist, der Geheimhaltung im gleichen und im gesetzlich möglichen Rahmen unterworfen werden.

3. Sämtliche vertraulichen Informationen bleiben Geschäfts- und Betriebsgeheimnisse und geistiges Eigentum der offenlegenden Vertragspartei. Lizenzen oder sonstige Rechte, gleich welcher Art, werden durch diese Vereinbarung nicht eingeräumt.

4. Unbeschadet der Verpflichtung zur Geheimhaltung behält sich jede Partei vor, die während der jeweiligen Besprechung von ihren Mitarbeitern entwickelten Ideen oder die in den von ihr anlässlich der jeweiligen Besprechung mitgeteilten Informationen enthaltenen Ideen oder den von ihrem stammenden Teil der erarbeiteten Arbeitsergebnisse zum Schutzrecht anzumelden. Falls von Mitarbeitern beider Parteien gemeinsam Ideen entwickelt werden, werden sich diese Parteien gesondert über deren Anmeldung zum Schutzrecht einigen. Die Parteien werden dabei auch die Anteile am Zustandekommen der jeweiligen gemeinsamen Idee, den Anmeldeverantwortlichen und eine Regelung für die Kostentragung festlegen.

5. Die Verpflichtung zur Geheimhaltung und Nichtverwertung der gegenseitig mitgeteilten vertraulichen Informationen entfällt, soweit diese

- der informierten Partei vor der Mitteilung nachweislich bekannt waren, oder
- der Öffentlichkeit vor der Mitteilung bekannt oder allgemein zugänglich waren, oder
- der Öffentlichkeit nach der Mitteilung ohne Mitwirkung oder Verschulden der informierten Partei bekannt oder allgemein zugänglich werden, oder
- im Wesentlichen Informationen entsprechen, die der informierten Partei zu irgendeinem Zeitpunkt von einem berechtigten Dritten offenbart oder zugänglich gemacht wurden.
- zur Wahrung von Rechtsansprüchen gegenüber Gerichten erforderlich ist oder kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens, die zur Offenlegung vertraulicher Informationen führen könnten, bestehen, wird die an dem Verfahren beteiligte Partei die andere Partei dieser Vertraulichkeitsvereinbarung hierüber unverzüglich informieren und eine Offenlegung der vertraulichen Information nicht ohne eine solche vorherige Information durchführen.

6. Die Geheimhaltungspflicht endet 3 (drei) Jahre nach Abbruch der Gespräche, Abbruch der Vertragsverhandlungen oder Beendigung einer eventuellen vertraglichen Zusammenarbeit der Parteien.

7. Die Parteien sind verpflichtet, alles Notwendige und Erforderliche zu unternehmen, um den unbefugten Zugriff Dritter auf die vertraulichen Informationen durch geeignete Vorkehrungen zu verhindern. Die vertraulichen Informationen, insbesondere in schriftlicher, visueller oder elektronischer Form bzw. deren Datenträger sind an einem gegen den unberechtigten Zugriff Dritter gesicherten Ort aufzubewahren. Insbesondere sind die Mitarbeiter/Berater der Parteien nachdrücklich auf die Einhaltung der vorliegenden Vertragsbedingungen sowie der Bestimmungen des Urheberrechts hinzuweisen.

8. Die Parteien werden die vertraulichen Informationen, die sie jeweils vom anderen Partner erhalten haben, nach Beendigung dieser Geheimhaltungspflicht unverzüglich an den Informationsgeber herausgeben.

9. Die Parteien verpflichten sich - soweit erforderlich - die Bestimmungen des Datenschutzes in der jeweils gültigen Fassung einzuhalten.

10. Im Falle einer Verletzung dieser Vereinbarung ist die verletzende der geschädigten Partei zum Schadensersatz verpflichtet. Die geschädigte Partei ist nach ihrer Wahl berechtigt, entweder Ersatz des entstandenen Schadens oder Zahlung einer Lizenz oder sonstigen Abgeltungsvergütung zu verlangen, die sonst für die zur Verfügung Stellung der Information zu zahlen gewesen wäre. Die Gesamthaftung jeder Partei für verursachte Schäden

bzw. für die Zahlung von Lizenzen oder sonstigen Abgeltungsvergütungen ist - unabhängig von der Anzahl der Verletzungs- bzw. Schadensfälle und unbeschadet von vorsätzlich herbeigeführten Schäden - auf maximal € 500.000,- beschränkt. Vorstehende Regelungen gelten auch bei Verstößen insbesondere durch Mitarbeiter oder Berater der Parteien.

11. Die offenlegende Partei übernimmt keine Garantie für die Richtigkeit und Geeignetheit der überlassenen vertraulichen Informationen. Die Haftung für hieraus resultierende Vermögensschäden wird im gesetzlich möglichen Rahmen ausgeschlossen.

12. Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland.

13. Für Streitigkeiten aus dieser Vereinbarung vereinbaren die Parteien Leipzig als ausschließlichen Gerichtsstand.

14. Dieser Text stellt die vollständige Vereinbarung dar. Mündliche Nebenabreden bestehen nicht. Änderungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses. Für die Einhaltung des Schriftformerfordernisses, auch für den Abschluss dieser Vereinbarung, ist die Verwendung einer qualifizierten elektronische Signatur gemäß Gesetz über Rahmenbedingungen für elektronische Signaturen ausreichend, mindestens jedoch erforderlich.

15. Im Falle der ganzen oder teilweisen Unwirksamkeit einzelner Klauseln der vorliegenden Vereinbarung verpflichten sich die Parteien, eventuell unwirksame Bestimmungen so umzudeuten, zu ergänzen oder zu ersetzen, dass der mit der unwirksamen Bestimmung verfolgte wirtschaftliche Zweck erreicht wird. Dasselbe gilt für den Fall, dass Regelungslücken in dieser Vereinbarung vorhanden sein sollten. Die deutsche Sprache dieser Vereinbarung hat Vorrang vor einer eventuell vorhandenen Übersetzung.

Teil 3 Vereinbarung zur Auftragsverarbeitung

Die Vereinbarung zur Auftragsverarbeitung findet Anwendung, wenn seitens DigiFors (nachfolgend „Auftragnehmer“) im Auftrag des Kunden („nachfolgend „Auftraggeber“) personenbezogene Daten weisungsgebunden verarbeitet werden. Insbesondere gilt das für folgende Dienstleistungen:

- SOC-Dienstleistungen
- Durchführung IT-forensischer Analysen
- Penetrationstests
- Übernahme eines Mandats zum Datenschutz- oder Informationssicherheitsbeauftragten
- E-Discovery Dienstleistungen

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1. Dauer des Auftrags

Der Vertrag beginnt am Tag der Auftragserteilung und läuft auf unbestimmte Zeit. Der Vertrag endet mit Beendigung des diesem zu Grunde liegenden Hauptvertrags.
Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftrag-gebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkenn-bar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind

gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

3. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sowie Weisungsempfänger beim Auftragnehmer werden mit Auftragsbestätigung mitgeteilt. In jedem Fall sind die jeweiligen gesetzlichen Vertreter (insb. Geschäftsführer) weisungsberechtigt bzw. Weisungsempfänger.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertrags-partner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

4. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hier-zu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftrag-geber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privat-wohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutz-rechtlichen Vorschriften der DSGVO bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personen-bezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt, dessen Kontaktdaten unter https://digifors.de/datenschutz/ veröffentlicht sind.

5. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer gestattet, Art. 28 Abs. 2 DSGVO. Beabsichtigt der Auftragnehmer die Beauftragung eines Subunternehmers, hat er diesen dem Auftraggeber mit Namen und Anschrift sowie der vorgesehenen Tätigkeit des Subunternehmers mitzuteilen (Ziff.4). Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
Der Auftragnehmer setzt folgende Subunternehmer ein, die personenbezogene Daten im Auftrag verarbeiten:

Adresse	Zweck
Microsoft Corporation, One Microsoft Way Redmond, WA 98052-6399 USA	M365(Office, Teams)
Twilio Inc., 101 Spear Street, Fifth Floor, San Francisco	Alarming per SMS

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen

Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

7. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

8. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format auf Verlangen zu bestätigen.

9. Haftung

Auf Art. 82 DSGVO wird verwiesen.

10. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Teil 3.1 Technische und organisatorische Maßnahmen (Stand 11.03.2025)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Vertraulichkeit im Sinne des Art. 32 Abs. 1 lit. b in Verbindung mit ErwGr 39 und 83 DS-GVO ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu Daten haben und weder Daten noch Geräte, mit denen diese verarbeitet werden, benutzen können und die Daten außerdem gemäß Art. 5 Abs. 1 lit. f DS-GVO vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind.

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

- Einrichtung von Sicherheitszonen
- Dokumentiertes Sicherheitszonenkonzept
- Räumliche Trennung von Besuchern und Mitarbeitenden
- Kein unbeaufsichtigter Zutritt zu sensiblen Bereichen möglich
- Schlüsselregelung und Quittierung der Schlüsselausgabe durch Assistenz der Geschäftsleitung

- Besucherregelungen
- Protokollierung der Besucher in Besucherliste am Haupteingang
- Gästeausweis für Besucher
- Begleitung von Besuchern durch interne Mitarbeitende in den Räumlichkeiten
- Verbot von Aufzeichnungen (Bild und Ton) für Besucher

- Technische Maßnahmen zur Zutrittskontrolle
- Alarmanlage der Schutzklasse C ist durch Versicherung abgenommen und wird regelmäßig extern gewartet
- Zugangskontrollsystem über Schlüssel und Dongle vorhanden
- Geschlossene Etagentür
- Manuelles Schließsystem
- Schließsystem mit unterschiedlichen Schlüsseln für einzelne Räumlichkeiten
- Videoüberwachung: Der interne Eingangsbereich wird außerhalb der Geschäftszeit per Video überwacht.
- Bewegungsmelder sind in der Alarmanlage integriert
- Sicherheitsschlösser, vorhandene Schließanlage nach anerkannten Regeln der Technik

- Dienstleisterregelungen
- Wachpersonal im Objekt vorhanden
- Die Alarmanlage ist zu einem separaten Wachdienst aufgeschaltet.
- Sorgfältige Auswahl des Reinigungspersonals, Reinigungspersonal hat keinen Zutritt zu den einzelnen Büros, da diese bei Abwesenheit immer verschlossen sind.

Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Technische Maßnahmen zur Zugangskontrolle
- Firewall (Hardware/Software) zentral auf Router und Server sowie dezentral an jedem Arbeitsplatz, verwendet werden kommerzielle Produkte mit aktiven Supportverträgen
- Firewall mit IDS
- AV für alle Geräte (Windows Defender)
- Einrichtung eines Benutzerstammsatzes pro User (Name, Benutzername, E-Mail, Rolle, Berechtigung, Policy)
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Authentifikation für Mitarbeitende über Nutzername / Passwort
- Authentifikation mit biometrischen Verfahren je nach Gerät
- Zwei-Faktor-Authentifizierung, wo möglich und vorhanden, gilt überwiegend für Services
- Passwortrichtlinie vorhanden sowie technisch erzwungener Passwortwechsel
- Automatische Bildschirmsperre bei Inaktivität
- Festplattenverschlüsselung von mobilen Endgeräten
- Auf Laptops/Notebook mit MS Windows wird Bitlocker default verwendet.
- Externe Datenträger werden mit BitLocker to Go verschlüsselt.
- tragbare Hochsicherheits-Festplatte HS128 der Firma Digitrade sind vorhanden und kommen bei Bedarf zum Einsatz
- Alle Geräte sind mit mindestens einer Siegeletikette versehen
- Zugriff für die Remoteeinwahl erfolgt per OpenVPN mit Zertifikat

- Organisatorische Maßnahmen zur Zugangskontrolle
- Anweisung Sperrung der Bildschirme nach Verlassen des Arbeitsplatzes
- Access Control Policy
- Rollen und Rechtekonzept vorhanden

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Authentifizierung
- Zentrales Identitätsmanagement über Entra
- Umsetzung Rollen und Rechtekonzept über Entra
- Verwaltung von Rechten erfolgt durch Systemadministration
- Geringe Anzahl von Administratoren (2 Administratoren und CEO)
- Trennung von Nutzer- und Administrationsaccounts
- Personalisierte Administrationsaccounts vorhanden
- Passwortrichtlinie vorhanden und dokumentiert
- Vier-Augen-Prinzip bei Bedarf bei Spezialanwendungen

- Protokollierung und Verschlüsselung
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten über SIEM-System
- Verschlüsselungsverfahren/-systeme nach anerkannten Regeln der Technik wo möglich
- Verwendung von Hashwert-Verfahren
- Bei Daten (Originaldaten), die uns übergeben werden, werden immer MD5 und SHA1 Prüfsummen gebildet, um die Datenintegrität nachweisen zu können.
- Verschlüsselung von Datenträgern
- Kryptografie-Richtlinie vorhanden

- Aufbewahrung, Löschung und Vernichtung
- Sichere Aufbewahrung von Datenträgern in Asservatenkammer
- physische Löschung von Datenträgern vor Wiederverwendung mindestens nach DoD 5220 mit Software Active KillDisk ausschließlich durch IT-Administration
- Ordnungsgemäße Vernichtung von Datenträgern und Akten (nach DIN 66399) über externen Dienstleister REISSWOLF
- Protokollierung der Vernichtung durch externen Dienstleister, Vernichtungsprotokolle werden aufbewahrt

Trennungskontrolle
Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten, getrennt verarbeitet werden.

- Physikalisch getrennte Speicherung von Daten auf gesonderten Systemen oder Datenträgern
- Netztrennung zwischen Officenetz und IT-Forensik
- Logische Mandantentrennung (softwareseitig), mindesten im Dateisystem

- Rollen- und Rechtekonzept vorhanden
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Trennung von Produktiv- und Testsystemen physisch oder per VLAN
- Sandboxing bei der Untersuchung, Analyse und/oder Bewertung von Software
- Protokollierung und Beweissicherung über SIEM-System

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Integrität im Sinne des Art. 32 Abs. 1 lit. b in Verbindung mit Art. 5 Abs. 1 lit. f DS-GVO ist gewährleistet, wenn Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt sind.

Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft oder festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Zugriff für die Remoteeinwahl erfolgt per OpenVPN mit Zertifikat
- E-Mail-Verschlüsselung per PGP
- Dokumentation der Abruf- und Übermittlungsprogramme wird im Azure Security Center abgebildet
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen im Verfahrensverzeichnis
- Datenträgerverwaltung/-kennzeichnung
- Verschlüsselung von Datenträgern
- Regelung / Dokumentation Ein- und Ausgang von Datenträgern und Empfängerkreis
- Fernwartungskonzept vorhanden, Umsetzung über Teamviewer

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Einsatz von Software die anerkannten Regeln der Technik entspricht
- Identitätsmanagement über Entra
- Protokollierung der Eingabe, Änderung und Löschung von Daten über SIEM
- Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten auf Basis Rollen- und Rechtekonzept

- Regelmäßige Berechtigungsprüfung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeit im Sinne des Art. 32 Abs. 1 lit. b DS-GVO ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss gemäß Art. 32 Abs. 1 lit. c DS-GVO die Fähigkeit bestehen die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können. Belastbarkeit ist gemäß Art. 32 Abs. 1 lit. b auf Dauer sicherzustellen und betrifft Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- AV für alle Geräte
- Firewall mit IDS
- Unterbrechungsfreie Stromversorgung (USV) vorhanden
- Klima- und Brandmeldeanlage im Serverraum
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen vorhanden
- Regelmäßige Brandschutzbegehung durch Externe in allen Räumlichkeiten
- Feuerlöschgeräte in Serverräumen vorhanden
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Alarmanlage der VDE- Schutzklasse C
- Bewegungsmelder vorhanden
- Glasbruchmelder an den Fenstern im Serverraum
- Dokumentiertes Backupkonzept
- Generationprinzip
- auf Band
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort

Wiederherstellbarkeit
Maßnahmen, die die rasche Wiederherstellung (Art. 32 Abs. 1 lit. c DS-GVO) der Verfügbarkeit von Daten nach deren zwischenzeitlichem Verlust oder Beschädigung gewährleisten.

- Dokumentiertes Backup- und Recovery-Konzepts
- Regelmäßiger Test der Datenwiederherstellung
- Notfallplan vorhanden
- Incident Response Plan vorhanden
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Organisation

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.

- Urlaubs- und Krankheitsvertretung der Geschäftsführung und des IT-Verantwortlichen
- Regelungen über Sicherung des Datenbestands
- Regelmäßige Hinweise an Mitarbeitende, um Problembewusstsein zu fördern
- Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen
- Dokumentation von Sicherheitsrichtlinien und Freigabe für alle Mitarbeitenden
- Einsatz eines ISMS nach ISO/IEC 27001:2022

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

Datenschutzmanagement
Integration eines Datenschutzmanagementsystems in das bestehende ISMS, um die Verfügbarkeit, Vertraulichkeit und Integrität personenbezogener Daten sicherzustellen.

- Freigegebene, dokumentierte Datenschutzrichtlinie
- Dokumentierte Prozesse zum Datenschutz
- Regelmäßige Überprüfung der TOMs
- Regelmäßige Datenschutzaudits
- Interner jährlicher Datenschutzbericht
- Jährliche Datenschutzschulung

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Privacy by design / Privacy by default

- Pseudonymisierung oder Anonymisierung von personenbezogenen Daten
- Beschränkung des Umfangs der Verarbeitung der erhobenen Daten, der Speicherfrist und der Zugänglichkeit

Auftragskontrolle
Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogene Daten nur nach Weisung des Auftraggebers verarbeitet werden können.

- Eindeutige Vertragsgestaltung / vertragliche Regelungen
- Formalisierte Auftragserteilung
- Strenge Auswahl des Dienstleisters (insbesondere hinsichtlich Datensicherheit)
- Risikobewertung von Dienstleistern
- Lieferantenrichtlinie vorhanden
- Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten (Kontrolle der Einhaltung)