Vereinbarung über Auftragsverarbeitung

zu den Idana-Diensten (insbesondere Idana und Idana Flow) zwischen der

Idana AG
Ellen-Gottlieb-Straße 19
79106 Freiburg im Breisgau
Deutschland

- nachfolgend "**Auftragsverarbeiter**" genannt -

und

der Praxis/der Klinik
(wie im Bestellformular bzw. bei der Registrierung des Idana-Zugangs angegeben)

- nachfolgend "**Verantwortlicher**" genannt -

1 Definitionen

Begriffsdefinitionen aus dem Bestellformular/-website von Idana, der Registrierungsseite des Idana-Zugangs, dem Idana-Kundenportal und den AGB (nachfolgend "Hauptvertrag" genannt) gelten auch für diese Vereinbarung über Auftragsverarbeitung (nachfolgend „AVV" genannt), soweit hierin nicht ausdrücklich etwas anderes bestimmt ist. Da die vorliegende AVV sowohl im Bereich der Datenschutz-Grundverordnung (DSGVO) als auch in dem des schweizerischen Bundesgesetz über den Datenschutz (DSG) Anwendung findet und die DSGVO für ein wesentlich größeres räumliches Anwendungsgebiet gilt, werden nachfolgend in der AVV die in der DSGVO definierten und in ihrem Anwendungsbereich gebräuchlichen Begriffe verwendet. Die „*Verarbeitung*" von „*personenbezogenen Daten*" sowie von „*personenbezogenen Daten besonderer Kategorie*" entspricht daher begrifflich dem „*Bearbeiten*" von „*Personendaten*" und „*besonders schützenswerten Personendaten*" nach dem DSG. Der „*Auftragsverarbeiter*" steht begrifflich dem „*Auftragsbearbeiter*" des DSG gleich und eine „*Verletzung des Schutzes personenbezogener Daten*" meint im Sinne des DSG eine „*Verletzung der Datensicherheit*". Weitere im DSG verwendete Begriffe, die bei vergleichbarer Bedeutung von denen in der DSGVO abweichen, werden bei der ersten Nennung des DSGVO-Pendants in Klammern angegeben, z.B. „(DSG: Personendaten)". Ungeachtet der Verwendung der Begriffe aus der DSGVO richtet sich die Begriffsbedeutung nach dem DSG, soweit dessen Anwendungsbereich betroffen ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Der Auftragsverarbeiter stellt dem Verantwortlichen nach Maßgabe des Hauptvertrages mittels Software-as-a-Service die Funktionen der Idana-Dienste, insbesondere der Standardsoftware Idana (inkl. der Website idana.app) sowie des KI-Dokumentationsassistenten Idana Flow (inkl. der Website app.idanaflow.com) bereit, übernimmt das Hosting von personenbezogenen Daten, überlässt dem Verantwortlichen Komponenten der Standardsoftware Idana und erbringt Support- und Softwarepflegeleistungen für die überlassene Standardsoftware bzw. die bereitgestellten Funktionen (nachfolgend zusammenfassend „Auftrag" genannt). Dabei kann nicht ausgeschlossen werden, dass der Auftragsverarbeiter Zugriff auf personenbezogene Daten erhält oder nehmen muss und bei Bereitstellung der Idana-Dienste solche Daten im Auftrag des Verantwortlichen verarbeitet. Der Auftragsverarbeiter verarbeitet die im Zusammenhang mit dem Auftrag stehenden personenbezogenen Daten ausschließlich im Rahmen der in dieser AVV getroffenen Bestimmungen. Der Auftragsverarbeiter verarbeitet die betreffenden personenbezogenen Daten für keine anderen und insbesondere nicht für eigene Zwecke.

2.2 Die Zwecke und Mittel der Verarbeitung bestimmt alleine der Verantwortliche. Änderungen des Verarbeitungsgegenstandes und Verarbeitungsänderungen sind gemeinsam abzustimmen und schriftlich oder in Textform (z.B. E-Mail) durch Änderung dieser AVV festzulegen.

2.3 Die Dauer dieser AVV (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

3 Konkretisierung des Auftrags

3.1 Der Inhalt des Auftrags wird in Bezug auf die Auftragsverarbeitung wie folgt konkretisiert:

Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung ergeben sich aus dem Gegenstand des Hauptvertrages. Übergeordneter Zweck ist die Bereitstellung der Funktionen der Idana-Dienste, insbesondere der Standardsoftware Idana und der Website idana.app mittels Software-as-a-Service, die Bereitstellung der Funktionen von Idana Flow (insb. Aufzeichnung, Transkription und KI-basierte Zusammenfassung von Arzt-Patienten-Gesprächen), das Hosting von personenbezogenen

Daten, die Überlassung von Softwarekomponenten, die Aufrechterhaltung des Betriebs einschließlich Betreuung und Wartung sowie die Erbringung von Entstörungs-, Support- und Softwarepflegeleistungen. Das Hosting betrifft unter anderem Patientendaten. Zu den Softwarepflegeleistungen gehören insbesondere die Beseitigung der vom Verantwortlichen gemeldeten Mängel der Standardsoftware sowie die Bereitstellung eines Hotline-Supports. Die Unterstützung erfolgt auch per Fernwartung.

Art der personenbezogenen Daten

Personen- und Patientenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten, Kunden- und Patientenhistorie, Vertragsabrechnungs- und Zahlungsdaten, besondere Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten (DSG: Daten über die Gesundheit), die mit den Idana-Diensten verarbeitet werden), Planungs- und Steuerungsdaten, Audio-Aufzeichnungen von Arzt-Patienten-Gesprächen (nur Idana Flow), Text-Transkripte und KI-generierte Zusammenfassungen von Gesprächen (nur Idana Flow).

Kategorien der betroffenen Personen

Kunden, Beschäftigte i. S. d. § 26 BDSG (DSG: Mitarbeiterinnen und Mitarbeiter), Patienten der Kunden.

3.2 Der Auftragsverarbeiter stellt dem Verantwortlichen in Idana zusätzlich programmgesteuerte Schnittstellen (API) bereit, über die der Verantwortliche - über eigene Systeme oder von ihm beauftragte Dienste Dritter (z. B. Anbieter von Onlineterminkalendern) - Stammdaten übermitteln, Befragungen auslösen und den Bearbeitungsstatus abrufen kann; Antwortinhalte sind über die API nicht abrufbar. Zur Klarstellung halten die Vertragspartner fest, dass zwischen dem Auftragsverarbeiter und dem vom Verantwortlichen mit der API-Nutzung gegebenenfalls beauftragten Dritten kein Vertrags- und Auftragsverhältnis besteht. Der Auftragsverarbeiter und der Dritte handeln dementsprechend parallel beide jeweils als Auftragsverarbeiter für den Verantwortlichen und nicht im Rahmen einer Kettenauftragsverarbeitung.

3.3 **Einsatz von zertifizierten Support-Partnern durch den Verantwortlichen**:

Sofern der Verantwortliche für die technische Anbindung und/oder den First-Level-Support der Idana-Dienste einen von Idana zertifizierten Partner („Support-Partner“) beauftragt, weist der Verantwortliche den Auftragsverarbeiter hiermit an, Supportanfragen und die damit verbundenen personenbezogenen Daten zur Bearbeitung an diesen Support-Partner weiterzuleiten (z.B. durch Ticket-Routing im System oder E-Mail in BCC). Der Verantwortliche stellt sicher, dass Supportanfragen keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO (insbesondere Gesundheitsdaten) enthalten. Der Verantwortliche kann diese Weisung in Textform (E-Mail an support@idana.com) widerrufen. Nach Eingang des Widerrufs leitet Idana keine weiteren Supportanfragen und die damit verbundenen personenbezogenen Daten an den Support-Partner weiter. Zur Klarstellung: Zwischen dem Auftragsverarbeiter und dem Support-Partner wird kein Unterauftragsverhältnis begründet; beide handeln parallel als eigenständige Auftragsverarbeiter für den Verantwortlichen.

4 Weisungsgebundenheit

4.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, bzw. im Anwendungsbereich des DSG durch das Recht der Schweiz hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung in Textform mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation.

4.2 Der Verantwortliche hat das Recht, dem Auftragsverarbeiter im Rahmen des Auftragsgegenstandes (siehe Ziffer 2) Weisungen hinsichtlich der Art, des Umfangs und des Verfahrens der Verarbeitung der personenbezogenen Daten zu erteilen. Seine Weisungen kann er durch Einzelweisungen konkretisieren. Mündlich erteilte Weisungen sind vom Auftragsverarbeiter unverzüglich schriftlich oder in Textform zu bestätigen. Als Weisung ist dabei die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Berichtigung, Einschränkung der Verarbeitung (DSG: Anbringung eines Bestreitungsvermerks), Löschung, Herausgabe) des Auftragsverarbeiters mit personenbezogenen Daten gerichtete Anordnung des Verantwortlichen zu verstehen. Die grundlegenden Weisungen betreffen den Betrieb und die Betreuung der mittels Software-as-a-Service zugänglich gemachten Funktionen der Idana-Dienste; sie ergeben sich aus dem Hauptvertrag und dieser Vereinbarung über Auftragsverarbeitung.

4.3 Der Verantwortliche hat alle Weisungen, die er dem Auftragsverarbeiter erteilt, zu dokumentieren. Die Dokumentation stellt er dem Auftragsverarbeiter für jede erteilte Weisung zur Verfügung. Für die Dokumentation der Umsetzung der vom Verantwortlichen erteilten Weisungen ist dagegen der Auftragsverarbeiter verantwortlich.

4.4 Den entsprechenden Weisungen des Verantwortlichen hat der Auftragsverarbeiter jederzeit Folge zu leisten. Solange und soweit der Auftragsverarbeiter personenbezogene Daten aus dem Auftrag über das Auftragsende hinaus

verarbeitet, gilt die Weisungsgebundenheit gegenüber dem Verantwortlichen auch nach der Beendigung dieser AVV weiter; Aufwendungen und Kosten, die dem Auftragsverarbeiter hierdurch entstehen, trägt der Verantwortliche.

4.5 Der Auftragsverarbeiter unternimmt alle erforderlichen Schritte, um sicherzustellen, dass die ihm unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten bzw. im Anwendungsbereich des DSG durch das Recht der Schweiz zur Verarbeitung verpflichtet.

4.6 Falls Weisungen die in Ziffer 3 getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn vorher eine entsprechende Änderung dieser AVV in Text- oder Schriftform erfolgt ist.

4.7 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, wenn eine vom Verantwortlichen erteilte Weisung nach Auffassung des Auftragsverarbeiters gegen gesetzliche Vorschriften und insbesondere gegen die DSGVO, das BDSG oder gegen andere anwendbare Datenschutzbestimmungen der Europäischen Union oder ihrer Mitgliedstaaten bzw. im Anwendungsbereich des DSG gegen das DSG verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Sofern der Auftragsverarbeiter darlegen kann, dass eine Verarbeitung nach Weisung des Verantwortlichen zu einer Haftung des Auftragsverarbeiters nach Art. 82 DSGVO führen kann, steht dem Auftragsverarbeiter das Recht zu, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Vertragspartnern auszusetzen.

5 Verpflichtung zur Vertraulichkeit

5.1 Der Auftragsverarbeiter gewährleistet, dass er bei der Verarbeitung personenbezogener Daten nur Mitarbeiter beschäftigt, die er mit den für sie maßgebenden Bestimmungen des Datenschutzrechtes vertraut gemacht und schriftlich oder elektronisch - auch über die Beendigung ihrer Tätigkeit hinaus - zur Vertraulichkeit verpflichtet hat. Einer Verpflichtung bedarf es nicht, wenn Mitarbeiter einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.2 Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften durch die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben. Seine mit der Verarbeitung von personenbezogenen Daten betrauten Mitarbeiter wird der Auftragsverarbeiter regelmäßig in angemessenem Umfang und in angemessenen Abständen schulen und für den Datenschutz sensibilisieren.

5.3 Der Verantwortliche ist verpflichtet, alle im Rahmen des Auftrags erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie Daten- und andere IT-Sicherheitsmaßnahmen des Auftragsverarbeiters, insbesondere die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters, streng vertraulich zu behandeln und diese weder weiterzugeben noch auf sonstige Art zu verwerten oder zu offenbaren. Dies gilt gegenüber jeglichen unbefugten Dritten, d.h. auch gegenüber eigenen unbefugten Mitarbeitern, sofern die Weitergabe bzw. sonstige Verwertung oder Offenbarung von solchen Informationen nicht zur ordnungsgemäßen Erfüllung der vertraglichen oder gesetzlichen Verpflichtungen des Verantwortlichen erforderlich ist. In Zweifelsfällen ist der Verantwortliche verpflichtet, vor einer solchen Weitergabe bzw. sonstigen Verwertung oder Offenbarung die schriftliche Zustimmung des Auftragsverarbeiters einzuholen.

5.4 Ungeachtet der in Ziffer 5.3 vereinbarten Verschwiegenheitspflichten des Verantwortlichen darf dieser technische und organisatorische Maßnahmen des Auftragsverarbeiters, die den Auftrag betreffen, im Rahmen der dem Verantwortlichen gesetzlich auferlegten Rechenschaftspflicht gegenüber berechtigten Personen und Stellen (z.B. Aufsichtsbehörden) offenbaren, soweit er dazu gesetzlich verpflichtet ist.

6 Wahrung berufsrechtlicher Geheimnisse

6.1 Dem Auftragsverarbeiter ist bewusst, dass ein erheblicher Teil der Mitarbeiter des Verantwortlichen aufgrund ihrer beruflichen Tätigkeit in einer Arztpraxis/Klinik oder in anderen medizinischen Einrichtungen mit besonders geschützten personenbezogenen Daten und Daten, die als Patientendaten unter die berufsrechtliche Verschwiegenheitspflicht fallen, arbeitet; dies betrifft auch die vom Auftragsverarbeiter im Zusammenhang mit dem Auftrag zu erbringenden Support- und Softwarepflegeleistungen. Das unbefugte Offenbaren solcher Daten ist nach Maßgabe der einschlägigen Bestimmungen des jeweils anwendbaren Strafrechts und Datenschutzrechts strafbar.

6.2 Daher gilt im Anwendungsbereich des deutschen Strafrechts folgende Verpflichtung auf das Privatgeheimnis (§ 203 StGB):

6.2.1 Der Auftragsverarbeiter gewährleistet, dass in seinem Verantwortungsbereich alle datenschutzrechtlichen Anforderungen eingehalten werden und dass die Verletzung des Privatgeheimnisses (§ 203 StGB) durch die Erfüllung seiner vertraglichen Pflichten aus dem Hauptvertrag und dieser AVV sowie aller damit im Zusammenhang stehenden Leistungen ausgeschlossen ist.

6.2.2 Der Auftragsverarbeiter verpflichtet seine Mitarbeiter vor ihrem erstmaligen Einsatz im Zusammenhang mit der Verarbeitung personenbezogener Daten aus dem Auftrag auf das Privatgeheimnis (§ 203 StGB). Die Verpflichtung der Mitarbeiter erfordert über die reine Verpflichtung hinaus eine Einweisung in die Bedeutung und die Rechtsfolgen, die sich aus § 203 StGB ergeben.

6.3 Im Anwendungsbereich des schweizerischen Strafrechts gilt folgende Verpflichtung auf das Berufsgeheimnis (Art. 321 StGB, Art. 62 DSG):

6.3.1 Der Auftragsverarbeiter verpflichtet sich, über Berufsgeheimnisse (Art. 321 StGB) Stillschweigen zu bewahren und sich nur insoweit Kenntnis von dem Berufsgeheimnis unterliegenden Daten zu verschaffen, wie dies zur Erfüllung seiner vertraglichen Pflichten aus dem Hauptvertrag und dieser AVV sowie aller damit im Zusammenhang stehenden Leistungen erforderlich ist.

6.3.2 Der Auftragsverarbeiter verpflichtet seine Mitarbeiter und die von ihm beigezogenen Dritten vor ihrem erstmaligen Einsatz im Zusammenhang mit der Verarbeitung personenbezogener Daten aus dem Auftrag auf das Berufsgeheimnis (Art. 321 StGB). Die Verpflichtung der Mitarbeiter erfordert über die reine Verpflichtung hinaus eine Einweisung in die Bedeutung und die Rechtsfolgen, die sich aus Art. 321 StGB und Art. 62 DSG ergeben.

6.4 Der Auftragsverarbeiter muss weitere Auftragsverarbeiter sorgfältig auswählen und diese auf die berufsrechtliche Verschwiegenheitspflicht verpflichten, soweit weitere Auftragsverarbeiter Zugriff auf Daten haben, die der berufsrechtlichen Verschwiegenheitspflicht unterliegen (§203 StGB bzw. Art. 321 StGB). Darüber hinaus müssen solche weiteren Auftragsverarbeiter das eingesetzte Personal ebenfalls zur Geheimhaltung verpflichten und über die Folgen einer Pflichtverletzung belehren. Dies gilt in der gesamten Beauftragungskette für alle weiteren Auftragsverarbeiter entsprechend.

7 Technische und organisatorische Maßnahmen

7.1 Der Auftragsverarbeiter setzt für den Auftrag unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten (DSG: Risiko für die Persönlichkeit oder die Grundrechte) der Betroffenen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser AVV erfolgt.

7.2 Die als Anhang 2 (Technische und organisatorische Maßnahmen) beigefügten Datenschutzvorkehrungen des Auftragsverarbeiters, die die Festlegungen gemäß Art. 32 DSGVO bzw. im Anwendungsbereich des DSG gemäß Art. 7 DSG enthalten, werden für die Durchführung des Auftrags als verbindliches Minimum festgelegt, das zu keiner Zeit unterschritten werden darf. Der Auftragsverarbeiter verpflichtet sich zur Einhaltung der in Anhang 2 niedergelegten technischen und organisatorischen Maßnahmen.

7.3 Stellt der Verantwortliche während der Laufzeit des Auftrages fest, dass sich die Risiken für die Rechte und Freiheiten der Betroffenen verändert haben, teilt er dies dem Auftragsverarbeiter unverzüglich mit, damit der Auftragsverarbeiter seine technischen und organisatorischen Maßnahmen so anpassen kann, dass das für den Auftrag erforderliche Datenschutzniveau weiterhin gewährleistet bleibt; die dem Auftragsverarbeiter durch die Anpassung entstehenden einmaligen und wiederkehrenden Aufwendungen und Kosten trägt der Verantwortliche. Sobald der Auftragsverarbeiter in Anhang 2 die aktualisierten technischen und organisatorischen Maßnahmen festgelegt hat, ersetzt dieser neue Anhang 2 den bis dahin gültigen Anhang 2. Sollte eine entsprechende Anpassung der technischen und organisatorischen Maßnahmen dem Auftragsverarbeiter nicht möglich, nicht zumutbar oder gar für ihn unzulässig sein, stellt dies für beide Vertragspartner einen wichtigen Grund dar, der zur außerordentlichen Kündigung des Hauptvertrages einschließlich der vorliegenden AVV berechtigt.

7.4 Der Auftragsverarbeiter stellt sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten von sonstigen Datenbeständen strikt getrennt werden. Nähere Anforderungen und Maßnahmen zur Trennung sind in den technischen und organisatorischen Maßnahmen in Anhang 2 festgelegt.

7.5 Wenn und soweit der Auftragsverarbeiter gegenüber dem Verantwortlichen zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen verpflichtet ist, kann er Nachweise über die Einhaltung genehmigter Verhaltensregelungen (DSG: Verhaltenskodizes) gemäß Art. 40 DSGVO bzw. im Anwendungsbereich des DSG gemäß Art. 11 DSG oder über aktuelle Zertifizierung gemäß Art. 42 DSGVO bzw. im Anwendungsbereich des DSG gemäß Art. 13 DSG vorlegen, um seinen Nachweis zu stützen. Des Weiteren kann er diesen Nachweis auch über aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter (DSG: Datenschutzberaterin oder -berater), IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch ein Informationssicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, als Bestandteil einer ISO 27001-Zertifizierung) führen.

7.6 Die technischen und organisatorischen Maßnahmen müssen im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Dazu werden die im Anhang 2 vereinbarten technischen und organisatorischen Maßnahmen vom Verantwortlichen und vom Auftragsverarbeiter im Lichte der Ziffer 7.1 sowie unter Berücksichtigung des Stands der Technik mindestens einmal im Kalenderjahr überprüft. Aus solchen Überprüfungen resultierende Änderungen sind in Textform festzulegen. Stellt der Auftragsverarbeiter während der Laufzeit des Auftrages von sich aus fest, dass die von ihm getroffenen Maßnahmen die Risiken für die Rechte und Freiheiten der Betroffenen nicht oder nicht mehr angemessen abdecken, benachrichtigt er den Verantwortlichen. Für die Anpassung des Anhangs 2 gelten die in Ziffer 7.3 vereinbarten Bestimmungen entsprechend.

8 Einbeziehung weiterer Auftragsverarbeiter

8.1 Der Verantwortliche erteilt hiermit seine allgemeine Zustimmung (DSG: vorgängige Genehmigung) zur Inanspruchnahme weiterer Auftragsverarbeiter.

8.2 Im Falle der Beauftragung von weiteren Auftragsverarbeitern (Kettenauftragsverarbeitung) oder der Ersetzung von weiteren Auftragsverarbeitern wird der Auftragsverarbeiter den Verantwortlichen informieren. Will der Verantwortliche gegen derartige Änderungen in Übereinstimmung mit Ziffer 8.5 Einspruch erheben, hat er diesen gegenüber dem Auftragsverarbeiter innerhalb von zwei (2) Wochen nach Zugang der Information bzw. unverzüglich nach Kenntniserlangung von einem sich später ergebenden Einspruchsgrund schriftlich zu erklären. Die Bestimmungen dieser Ziffer 8 gelten entsprechend für jede Hinzuziehung bzw. Ersetzung von weiteren Auftragsverarbeitern im Rahmen einer mehrstufigen Kettenauftragsverarbeitung.

8.3 Der Auftragsverarbeiter erlegt weiteren Auftragsverarbeitern im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats bzw. im Anwendungsbereich des DSG nach dem Recht der Schweiz im Wesentlichen dieselben Datenschutzpflichten auf, die in dieser AVV zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Dabei ist sicherzustellen, dass geeignete technische und organisatorische Maßnahmen auch von dem weiteren Auftragsverarbeiter so durchgeführt werden, dass die Verarbeitung den gesetzlichen Anforderungen des Datenschutzrechtes entspricht.

8.4 Bei Abschluss dieser AVV hat der Verantwortliche der Inanspruchnahme der in Anhang 1 (Weitere Auftragsverarbeiter) mit Namen und konkretisiertem Auftragsinhalt bezeichneten weiteren Auftragsverarbeitern mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang zugestimmt.

8.5 Der Verantwortliche kann gegen den Einsatz eines weiteren Auftragsverarbeiters durch den Auftragsverarbeiter nur dann Einspruch erheben, wenn er begründete Zweifel daran hat, dass der weitere Auftragsverarbeiter die datenschutzrechtlichen Bestimmungen oder die Bedingungen dieser Vereinbarung über Auftragsverarbeitung einhalten wird. Erhebt der Verantwortliche gegen einen weiteren Auftragsverarbeiter in zulässiger Weise Einspruch, wird der Auftragsverarbeiter zumutbare Anstrengungen unternehmen, um dem Verantwortlichen eine Änderung der Leistungen anzubieten oder eine wirtschaftlich angemessene Änderung der Konfiguration oder Nutzung der Leistungen durch den Verantwortlichen zu empfehlen, um die Verarbeitung personenbezogener Daten durch den beanstandeten weiteren Auftragsverarbeiter zu vermeiden, ohne den Verantwortlichen unangemessen zu belasten. Wenn der Auftragsverarbeiter nicht in der Lage ist oder es ihm nicht zumutbar ist, eine solche Änderung innerhalb eines angemessenen Zeitraums, der dreißig (30) Tage nicht überschreiten darf, zur Verfügung zu stellen, kann jeder Vertragspartner nach billigem Ermessen (i) den Hauptvertrag nur in Bezug auf diejenigen Dienstleistungen, die vom Auftragsverarbeiter nicht ohne den Einsatz des beanstandeten weiteren Auftragsverarbeiters erbracht werden können, oder (ii) den gesamten Hauptvertrag außerordentlich kündigen. In Bezug auf gekündigte Leistungen erstattet der Auftragsverarbeiter dem Verantwortlichen zeitanteilig die im Voraus für die Restlaufzeit der Beauftragung bzw. des gesamten Hauptvertrags gezahlten Vergütungen.

8.6 Nicht als Inanspruchnahme weiterer Auftragsverarbeiter im Sinne dieser Ziffer 8 sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Reinigungskräfte, Telekommunikationsleistungen und Postdienste.

9 Unterstützung des Verantwortlichen

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Pflicht, Anträge auf Wahrnehmung der in Art. 12 bis 22 DSGVO sowie in §§ 32 bis 37 BDSG bzw. im Anwendungsbereich des DSG in Art. 25 bis 32 DSG genannten Rechte der betroffenen Person zu bearbeiten und zu beantworten. Dazu wird er dem Verantwortlichen auf Anfrage alle zweckdienlichen Informationen bereitstellen, die dem Auftragsverarbeiter im Einzelfall vorliegen. Wendet sich ein Betroffener mit Anträgen auf Wahrnehmung der in Art. 12 bis 22 DSGVO und in §§ 32 bis 37 BDSG bzw. im Anwendungsbereich des DSG in Art. 25 bis 32 DSG genannten Rechten unmittelbar an den Auftragsverarbeiter, wird dieser den Betroffenen an den Verantwortlichen verweisen.

9.2 Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

9.3 Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um den Verantwortlichen gemäß Ziffer 9.1 unterstützen zu können.

9.4 Des Weiteren unterstützt der Auftragsverarbeiter mit den ihm zur Verfügung stehenden Informationen den Verantwortlichen bei dessen Einhaltung der ihm gemäß Art. 32 bis 36 DSGVO bzw. im Anwendungsbereich des DSG in Art. 8, 22 bis 24 DSG obliegenden Pflichten.

9.5 Der Verantwortliche verpflichtet sich, alle Aufwendungen und Kosten zu erstatten, die dem Auftragsverarbeiter im Rahmen der Unterstützung des Verantwortlichen entstehen, vorausgesetzt, der Auftragsverarbeiter hat den Verantwortlichen vorab über die ungefähre Höhe dieser Kosten informiert.

10 Rückgabe und Löschung von Daten

10.1 Nach Beendigung der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche im Zusammenhang mit dem Auftrag in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungsergebnisse, die personenbezogene Daten enthalten, sowie alle im Rahmen der Erbringung der Softwarepflegeleistungen verarbeiteten personenbezogenen Daten ohne vorherige Übergabe datenschutzgerecht zu löschen. Der Verantwortliche kann vom Auftragsverarbeiter jedoch verlangen, dass dieser ihm vor der Löschung die Unterlagen, Verarbeitungsergebnisse und personenbezogenen Daten übergibt und erst danach die Löschung des beim Auftragsverarbeiter verbliebenen Rests der personenbezogenen Daten durchführt. Die vorstehende Übergaberegelung ist so zu verstehen, dass der Verantwortliche nach erfolgter Übergabe über alle personenbezogenen Daten aus und im Zusammenhang mit dem Auftrag verfügt. Test- und Ausschussmaterial ist zu vernichten oder dem Verantwortlichen auszuhändigen.

10.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Gleiches gilt, soweit nach dem Unionsrecht oder dem vom Auftragsverarbeiter anzuwendenden Recht der Mitgliedstaaten bzw. im Anwendungsbereich des DSG nach dem Recht der Schweiz eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

10.3 Sollten nach Beendigung der vertraglichen Arbeiten zusätzliche Aufwendungen oder Kosten durch die Rückgabe, Vernichtung oder Löschung von personenbezogenen Daten entstehen, verpflichtet sich der Verantwortliche zur Erstattung dieser Kosten, vorausgesetzt, der Auftragsverarbeiter hat den Verantwortlichen vorab über die ungefähre Höhe dieser Kosten informiert. Es wird jedoch klargestellt, dass diese Kostenregelung nicht auf die automatisierte Löschung des Kundenaccounts und der zugehörigen Patientendaten nach der Kündigung des Idana-Abonnements anwendbar ist. Diese Leistung ist in den vertraglichen Arbeiten inkludiert.

10.4 Verarbeitet der Auftragsverarbeiter Kopien personenbezogener Daten im Rahmen der Wartung der mittels Software-as-a-Service zugänglich gemachten Funktionen der Idana-Dienste (einschließlich Entstörung und Support), so löscht er diese Daten unverzüglich, nachdem die Entstörung oder die Bearbeitung der Supportanfrage erfolgreich abgeschlossen ist.

11 Nachweis der Einhaltung der datenschutzrechtlichen Pflichten

11.1 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser AVV niedergelegten Pflichten zur Verfügung.

11.2 Außerdem ermöglicht und unterstützt der Auftragsverarbeiter Überprüfungen einschließlich Inspektionen und Untersuchungen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer oder von Aufsichtsbehörden durchgeführt werden. Der Auftragsverarbeiter erklärt sich insbesondere damit einverstanden, dass der Verantwortliche oder ein von diesem beauftragter Prüfer im Regelfall nach angemessener Vorankündigung berechtigt ist, während der üblichen Bürozeiten des Auftragsverarbeiters die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen dieser AVV im erforderlichen Umfang und ohne Störung des Betriebsablaufs des Auftragsverarbeiters vor Ort zu kontrollieren.

11.3 Sollte der durch den Verantwortlichen beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen Prüfer ein Einspruchsrecht.

12 Verzeichnis von Verarbeitungstätigkeiten (DSG: Verzeichnis der Bearbeitungstätigkeit)

12.1 Der Auftragsverarbeiter führt das gemäß Art. 30 Abs. 2 DSGVO bzw. im Anwendungsbereich des DSG gemäß Art. 12 DSG von ihm zu führende Verzeichnis und stellt dieses der Aufsichtsbehörde auf Anfrage zur Verfügung.

13 Sonstige Pflichten des Auftragsverarbeiters

13.1 Der Auftragsverarbeiter arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

13.2 Ist für eine geplante Verarbeitung personenbezogener Daten eine Datenschutz-Folgenabschätzung erforderlich, unterstützt der Auftragsverarbeiter den Verantwortlichen auf Anforderung bei der Durchführung und stellt ihm alle erforderlichen Dokumentationen und zweckdienlichen Informationen zur Verfügung. Für seinen damit verbundenen Aufwand verpflichtet sich der Verantwortliche zur Erstattung, vorausgesetzt, der Auftragsverarbeiter hat den Verantwortlichen vorab über die ungefähre Höhe dieser Kosten informiert.

13.3 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO bzw. im Anwendungsbereich des DSG gemäß Art. 49 bis 53 DSG sowie über Ermittlungen, die eine zuständige Behörde nach Art. 83 DSGVO und §§ 42, 43 BDSG bzw. im Anwendungsbereich des DSG nach Art. 65 DSG beim Auftragsverarbeiter durchführt, informieren, soweit diese Kontrollhandlungen, Maßnahmen oder Ermittlungen Bezüge zur Auftragsverarbeitung aufweisen.

14 Mitzuteilende Verstöße

14.1 Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich (DSG: so rasch als möglich), wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird. Meldungen erfolgen in Textform und müssen mindestens die in Art. 33 Abs. 3 DSGVO bzw. im Anwendungsbereich des DSG in Art. 24 Abs. 2 DSG aufgezählten Informationen umfassen.

14.2 Dem Auftragsverarbeiter ist bekannt, dass nach Art. 33 und 34 DSGVO Melde- und Benachrichtigungspflichten im Falle der Verletzung des Schutzes personenbezogener Daten gegenüber der Aufsichtsbehörde und den betroffenen Personen bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Verantwortlichen mitzuteilen. Der Auftragsverarbeiter hat in Abstimmung mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

14.3 Soweit den Verantwortlichen Pflichten nach Art. 33 und 34 DSGVO bzw. im Anwendungsbereich des DSG nach Art. 24 DSG treffen, hat der Auftragsverarbeiter ihn hierbei gegen Vergütung des für den Auftragsverarbeiter damit verbundenen Aufwandes zu unterstützen. Die Vergütungspflicht besteht nicht, wenn eine Unterstützung aufgrund eines Verstoßes des Auftragsverarbeiters gegen seine Pflichten als Auftragsverarbeiter erforderlich wird. Ungeachtet dessen bleibt der Verantwortliche für die Erfüllung der ihn gemäß Art. 33 und 34 DSGVO bzw. im Anwendungsbereich des DSG gemäß Art. 24 DSG treffenden Melde- und Benachrichtigungspflichten selbst verantwortlich.

15 Anhänge

Die folgenden Anhänge bilden einen wesentlichen Bestandteil dieser AVV und haben im Fall von Widersprüchen oder Unklarheiten Vorrang vor den Bestimmungen der vorliegenden AVV:

- **Anhang 1**: Weitere Auftragsverarbeiter
- **Anhang 2**: Technische und organisatorische Maßnahmen

Anhang 1: Weitere Auftragsverarbeiter

Name / Firma, Anschrift	Auftragsinhalt	Umfang der Auftragsverarbeitung	Zertifiziert nach
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Server-Infrastruktur für Idana inkl. Websites, Datenbanken, Backups, Logs	Verarbeitung von Patientendaten (im Rechenzentrum in Frankfurt, Backups/FailOver in Berlin). Die genutzten Dienste sind HIPAA-konform und zum Schutz von Gesundheitsdaten geeignet.	Anforderungskatalog Cloud Computing (C5) vom Bundesamt für Sicherheit in der Informationstechnik, ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DSS, HITRUST CSF, CSA STAR, FIPS 140-2 und weitere [Quelle]

Name / Firma, Anschrift	Auftragsinhalt	Umfang der Auftragsverarbeitung	Zertifiziert nach
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Bereitstellung von KI-Diensten (Large Language Models und Foundation Models). **Die übermittelten Daten werden nicht zum Trainieren von KI-Modellen verwendet oder gespeichert.**	Verarbeitung von Inhalten (z.B. Fragebogen-Antworten bei Idana; Audio-Daten/Transkripte bei Idana Flow) zur Erstellung von KI-basierten Zusammenfassungen, Transkriptionen oder Analysen (Verarbeitung ausschließlich innerhalb der Europäischen Union via Gemini Enterprise Agent Platform; es erfolgt keine Übermittlung in Drittländer).	Anforderungskatalog Cloud Computing (C5) vom Bundesamt für Sicherheit in der Informationstechnik, ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DSS, HITRUST CSF, CSA STAR, FIPS 140-2 und weitere [Quelle]
Amazon Web Services EMEA SARL (AWS), 38 avenue John F. Kennedy, L-1855, Luxemburg	Automatisierter E-Mail-Versand	Verarbeitung von Patientendaten und E-Mail-Versand (im Rechenzentrum in Frankfurt, für das AWS HIPAA-Compliance zum Schutz von Gesundheitsdaten bestätigt)	Anforderungskatalog Cloud Computing (C5) vom Bundesamt für Sicherheit in der Informationstechnik, ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DSS, HITRUST CSF, CSA STAR, FIPS 140-2 und weitere [Quelle]
TeamViewer Germany GmbH, Jahnstr. 30, 73037 Göppingen, Deutschland	Tools für Fernwartung und Fernzugriff	Verarbeitung der Video- und Audioübertragung während der Fernwartung	ISO 27001, ISO 9001, SOC 2, HIPAA/HITECH [Quelle]
AnyDesk Software GmbH, Türlenstraße 2, 70191 Stuttgart, Deutschland	Tools für Fernwartung und Fernzugriff	Verarbeitung der Video- und Audioübertragung während der Fernwartung	ISO 27001 [Quelle]
Friendly Captcha GmbH, Am Anger 3-5, 82237 Woerthsee, Deutschland	Anti-Bot und Spam-Schutz Dienst	Schutz von Webseiten und Online-Diensten vor Spam und Missbrauch durch Einsatz eines Proof-of-Work Verfahrens	-

Alle vom Auftragsverarbeiter eingesetzten weiteren Auftragsverarbeiter haben ihre eigenen Beschäftigten zur Geheimhaltung bei der Verarbeitung personenbezogener Daten verpflichtet.

Anhang 2 : Technische und organisatorische Maßnahmen

1 Pseudonymisierung und Verschlüsselung

1.1 Ziel: Erschwerung oder Verhinderung der Zuordnung von personenbezogenen Daten zu einer identifizierbaren Person durch Unberechtigte

1.2 Maßnahmen: - Pseudonymisierungsverfahren werden nicht angewendet, weil im Rahmen der Wartung der Standardsoftware, insbesondere im Supportfall, regelmäßig Datensätze benötigt oder eingesehen werden, die stets in Bilder oder Dokumente eingebettete Patientendaten enthalten. - Technische Verschlüsselungsverfahren finden auf allen Desktop-PCs sowie Laptops Anwendung. - Patienten-Antworten inkl. Bilder und Unterschrift werden mit einer echten (clientseitigen) Ende-zu-Ende-Verschlüsselung verschlüsselt (sog. “Zero-Knowledge-Technologie”). Mit dieser wird sichergestellt, dass nur der Empfänger der Daten - nämlich die Praxis - diese lesen kann. Die Ende-zu-Ende-Verschlüsselung nutzt eine Idana-eigene Private-/Public-Key-Infrastruktur. Das Schlüsselpaar wird bei der Account-Registrierung zufällig generiert und der private Schlüssel mit der sogenannten Entschlüsselungs-PIN geschützt, welche die Praxis bei der Account-Registrierung vergibt. Der private Schlüssel und die PIN werden niemals über das Internet übertragen. So ist die Entschlüsselung der damit geschützten Daten nur lokal auf dem Praxisrechner

möglich. Libsodium wird in Idana als kryptographische Bibliothek verwendet. Details zu den Algorithmen findet man unter: https://libsodium.gitbook.io/doc/ in den Kapiteln „Secret-key Cryptography / Authenticated Encryption“ und „Public-key Cryptography / Authenticated Encryption“. Als Algorithmus zur Schlüsselableitung aus der PIN kommt Argon2 zum Einsatz. Die kryptografischen Algorithmen entsprechen dem Stand der Technik und nutzen 256-bit Schlüssellänge.

1.3 Bei der Nutzung von KI-Funktionen innerhalb von Idana (diese sind in der Benutzeroberfläche stets als solche gekennzeichnet) werden die zur Verarbeitung notwendigen Daten (z.B. bereinigte Fragebogen-Antworten) flüchtig an die KI-Schnittstelle (Gemini Enterprise Agent Platform) übermittelt. Es erfolgt keine dauerhafte Speicherung dieser Daten auf der Server-Infrastruktur des Auftragsverarbeiters über den Verarbeitungsvorgang hinaus. Patientenstammdaten werden nicht an die KI-Schnittstelle übermittelt.

1.4 Bei der Nutzung von Idana Flow werden die Gesprächsinhalte (Audio-Daten) von der Web-Applikation verschlüsselt an das Cloud-Backend übertragen und von dort zur Verarbeitung (z.B. Transkription, Zusammenfassung) an die KI-Schnittstelle (Gemini Enterprise Agent Platform) weitergeleitet. Die Verarbeitung der Audio-Daten sowie die KI-Verarbeitung erfolgen flüchtig; es erfolgt keine dauerhafte Speicherung der Audio-Daten auf der Server-Infrastruktur des Auftragsverarbeiters, und bei der KI-Schnittstelle werden weder Audio-Daten noch Transkripte noch KI-Ergebnisse gespeichert oder für das Training von KI-Modellen verwendet. Das Verarbeitungsergebnis (Transkript und daraus erzeugte Dokumente, z.B. Arztbericht, Patienteninformation) wird an die Web-Applikation zurückgesendet. Soweit diese Ergebnisse zur Bereitstellung der Funktion (z.B. zur späteren Übernahme in das Praxisverwaltungssystem) auf der Server-Infrastruktur des Auftragsverarbeiters gespeichert werden, erfolgt dies ausschließlich clientseitig Ende-zu-Ende-verschlüsselt (Zero-Knowledge, vgl. Ziffer 1.2). Der Auftragsverarbeiter hat keinen Zugriff auf die Klartextinhalte. Die Speicherung erfolgt für maximal sieben Tage. Patientenstammdaten werden nicht an die KI-Schnittstelle übermittelt.

2 Zutrittskontrolle

2.1 Ziel: Unbefugten Personen wird der physische Zugang durch entsprechende Maßnahmen verwehrt.

2.2 Maßnahmen: - Der äußere Zugang in das Gebäude ist außerhalb der normalen Verkehrszeiten nur mit Schlüssel möglich. - Der Zugang in die Geschäftsräume (innerhalb des Bürogebäudes) ist ausschließlich durch eine abschließbare Tür möglich. - Personen, die keinen Schlüssel besitzen, können während der Arbeitszeiten nur Zutritt erlangen, wenn die Tür durch einen Mitarbeiter geöffnet wird. - Der Eingang zu den Geschäftsräumen wird videoüberwacht. - Die Vergabe von Büroschlüsseln ist entsprechend intern geregelt und dokumentiert. - Netzwerkschränke sind durch abschließbare Türen zusätzlich gesichert.

3 Zugangskontrolle

3.1 Ziel: Zugriffe auf das Unternehmensnetzwerk sind vor einer nicht autorisierten Nutzung zu schützen.

3.2 Maßnahmen: - Zugriffe auf Unternehmensressourcen sind mit Benutzerrollen und Gruppenrichtlinien geregelt. - Im Unternehmen ist eine Kennwortrichtlinie bzgl. Länge, Komplexität und Gültigkeitsdauer etabliert. Die Weitergabe von Kennwörtern ist untersagt. - Sperrungen (z.B. Kennwort oder Pausenschaltung) werden durch Unternehmensrichtlinien vorgegeben. - Alle Personen greifen über eine eindeutige Kennung (User ID) auf das Unternehmensnetzwerk zu. Werden zusätzliche Systeme zur Datenverarbeitung eingesetzt, besitzen diese u.U. eigene Zugriffskontrollen, diese werden ebenfalls durch entsprechende Maßnahmen abgesichert. - Eine 2-Faktor-Authentifizierung wird eingesetzt, wenn verfügbar. - Gruppenpasswörter werden auf relevanten Systemen nicht angewandt. - Das Unternehmensnetzwerk ist durch entsprechende Firewalls von und zum Internet geschützt. - Aktuelle Virenscanner werden auf allen relevanten Windows-Systemen eingesetzt.

4 Zugriffskontrolle

4.1 Ziel: Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

4.2 Maßnahmen: - Jedem Benutzer wird der Zugriff nur auf diejenigen Programme und Daten gewährt, die er zur Erledigung seiner Pflichten benötigt. - Alle produktiven Server werden in sicheren Rechenzentren oder im sicheren Serverraum betrieben.

5 Weitergabekontrolle

5.1 Ziel: Aspekte der Weitergabe personenbezogener Daten sind zu regeln, wie z.B. elektronische Übertragung, Datentransport und Übermittlungskontrolle.

5.2 Maßnahmen:

- Für die elektronische Weitergabe bzw. Übertragung von Daten, z.B. im Rahmen eines Remote-Supports, wird immer ein verschlüsselter Übertragungsweg verwendet. Dies gilt sowohl für die physische als auch für die netzwerkbasierte Datenübertragung.

6 Eingabekontrolle

6.1 Ziel: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

6.2 Maßnahmen:

- Die eingesetzten DV-Systeme protokollieren die erfolgten Datenzugriffe (Erstellung, Änderung, Löschung), abhängig vom DV-System.

7 Auftragskontrolle

7.1 Ziel: Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten.

7.2 Maßnahmen: - Die Auftragsverarbeitung erfolgt ausschließlich im Rahmen einer eindeutigen Vertragsgestaltung. Dies gilt auch für die Auftragsverarbeitung, in der die Idana AG als Verantwortlicher tätig ist (z.B. durch externe Firmen oder Partner). - Die Idana AG setzt bei der Verarbeitung ausschließlich Mitarbeiter ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. - Die Einhaltung der Vorgaben wird regelmäßig kontrolliert.

8 Verfügbarkeitskontrolle

8.1 Ziel: Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

8.2 Maßnahmen: - Die Idana AG verfügt über einen regelmäßigen Backup-Prozess. - Zugesandte Medien von Auftraggebern, die personenbezogene Daten enthalten, werden nach der Eingangskontrolle separat sicher aufbewahrt.

9 Trennungskontrolle

9.1 Ziel: Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

9.2 Maßnahmen: - Es werden die technischen Möglichkeiten der IT-Systeme genutzt, um die Trennung von personenbezogenen Daten zu ermöglichen, die von verschiedenen Auftraggebern stammen und/oder zu verschiedenen Zwecken erhoben werden. - Daten aus verschiedenen Unternehmensbereichen werden auf unterschiedlichen Bereichen der Server mit entsprechenden Zugriffsberechtigungen abgelegt. - Wenn im Rahmen eines Supportfalls des Auftraggebers personenbezogene Daten benötigt werden, werden diese entsprechenden Daten dieser Meldung zugeordnet und nur zur Bearbeitung der Meldung verwendet; für die Bearbeitung anderer Meldungen findet kein Zugriff auf diese Daten statt.

10 Verfahren zur regelmäßigen Überprüfung der Wirksamkeit

10.1 Ziel: laufende, sich an Änderungen der Rahmenbedingungen anpassende Sicherheit der Verarbeitung

10.2 Maßnahmen: - Im Rahmen dieser Vereinbarung sind zwischen den Parteien regelmäßige Überprüfungen vereinbart (siehe Ziffer 7.6 der AVV). - Im Rahmen der regelmäßigen Datenschutzbesprechungen, die durch den Datenschutzbeauftragten durchgeführt werden, werden entsprechende notwendige Änderungen bewertet, die Wirksamkeit der aktuellen Vereinbarungen bzw. der Maßnahmen und Prozesse geprüft.