Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO

V 1.5.3 D - EU/ EWR

Bitte dieses Dokument nicht heften, da es automatisiert digitalisiert wird.

Bitte beachten Sie die Kontaktdaten ihres Ansprechpartners.

Bitte dieses Dokument nicht heften, da es automatisiert digitalisiert wird.

Bitte beachten Sie die Kontaktdaten ihres Ansprechpartners.

Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO

zwischen

Firma: NEXUS / DIGITAL PATHOLOGY GmbH

Straße: Irmastraße 1

Ort: 78166 Donaueschingen

Vertreten durch: K. Fritsch, A. Giebisch, A. Liman, M. Schaaf

(Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt)

Bitte beachten Sie bei der Kommunikation, die ggf. abweichenden Kontaktdaten Ihres Ansprechpartners für diesen Vertrag:

Name:_____ E-Mail:_____ Telefonnummer:_____

Postanschrift:_____

und

Firma:_____

Straße :_____

Ort :_____

Vertreten durch:_____

(Nachfolgend „Auftraggeber“ genannt)

Bitte beachten Sie bei der Kommunikation die ggf. abweichenden Kontaktdaten Ihres Ansprechpartners für diesen Vertrag:

Name:_____ E-Mail:_____ Telefonnummer:_____

Postanschrift:_____

Inhaltsverzeichnis

1. Präambel 6

2. Verantwortlichkeit 6

3. Dauer des Auftrags 6

4. Weisungsbefugnis des Auftraggebers 7

5. Leistungsort 7

6. Pflichten des Auftragnehmers 8

7. Fernzugriff auf Systeme des Auftraggebers bei Prüfung/Wartung oder anderen Dienstleistungen über Fernzugriffe 10

8. Pflichten des Auftraggebers 10

9. Kontrollrechte des Auftraggebers 11

10. Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern 12

11. Unterauftragnehmer 13

12. Zurückbehaltungsrecht 14

13. Haftung 14

14. Schriftformklausel 15

15. Salvatorische Klausel 15

16. Rechtswahl, Gerichtsstand 16

Anlage 1 17

Nexus Auftragsverarbeitungsvertrag im Unternehmensverbund 17

17. Hauptvertrag 17

17.1. Leistungen 17

18. Auftragsverarbeitungsvertrag 17

18.1. Laufzeit des Auftragsverarbeitungsvertrages 18

18.2. Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind: 18

18.3. Weisungsempfänger beim Auftragnehmer sind: 19

18.4. Ort der vertraglichen Leistungserbringung 19

18.5. Datenschutzbeauftragter des Auftragnehmers 20

18.6. Datenschutzbeauftragter des Auftraggebers 20

18.7. Fernzugriff auf Systeme des Auftraggebers 20

18.8. Datenarten, Zwecke der Verarbeitung und Kreis der Betroffenen 21
18.8.1. Art der Daten 21
18.8.2. Zweck der Datenverarbeitung 22
18.8.3. Kreis der Betroffenen 23
18.9. Unterauftragnehmer 24
18.9.1. Verbunde Unternehmen des Auftragnehmers 24
18.9.2. Sonstige Unterauftragnehmer des Auftragnehmers 25
18.9.3. Unterauftragnehmer beim Auftragnehmer für Nebendienstleistungen 26
18.9.4. Verbundene Unternehmen des Auftraggebers 26

19. Gültige Rechtsnormen 27
19.1. Europa und europäischer Wirtschaftsraum (EU/ EWR) 27
19.2. Deutschland 27

20. Technische und organisatorische Maßnahmen 29
20.1. Zutrittskontrolle 29
20.2. Zugangskontrolle 29
20.3. Zugriffskontrolle 29
20.4. Integrität 30
20.5. Verfügbarkeit/ Wiederherstellung 30
20.6. Belastbarkeit 30
20.7. Pseudonymisierung/ Anonymisierung 30
20.8. Transportkontrolle/ Übertragungskontrolle/ Weitergabekontrolle 31
20.9. Regelmäßige Überprüfungen 31
20.10. Auftragskontrolle 31
20.11. Datenportabilität 32
20.12. Trennbarkeit 32
20.13. Löschbarkeit 32
20.14. Auskunft an Betroffene 33

Anlage 2 34

21. Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203 und 204 StGB (D) 34

Anlage 3 35

22. Zusatzvereinbarung evangelisches Datenschutzgesetz (EKD) (D) 35

Anlage 3 36

23. Zusatzvereinbarung katholisches Datenschutzgesetz (KDG) (D) 36

Allgemeiner Hinweis

Diese Vertragsvorlage beruht auf einer Mustervorlage, die in Zusammenarbeit der BvD e.V., bvitg, gmds, Deutsche Krankenhaus Gesellschaft und GDD erstellt wurde und ist nach CC-BY-SA 4.0 lizensiert. (https://www.bvitg.de/pressemitteilung-bvitg-050717/)

Im Dokument wird aus Gründen der Lesbarkeit durchgängig die männliche Form verwendet. Wenn beispielsweise von "Benutzern" gesprochen wird, sollen dennoch alle Geschlechter angesprochen sein.

1. Präambel

Dieser Auftragsverarbeitungsvertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien bei der Verarbeitung von personenbezogenen Daten im Auftrag. Nach dem in Kapitel 17 benannten Vertrag („Hauptvertrag“) und ggf. seinen Vertragsanlagen ist es erforderlich, dass der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet, für die der Auftragnehmer nicht als datenschutzrechtlich Verantwortlicher fungiert. Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag und seine Vertragsanlagen oder den Leistungen, die im vorliegenden Vertrag beschrieben sind, in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

Es gelten die Begriffsbestimmungen aus den in Kapitel 19 angegeben gültigen Rechtsnormen für den Datenschutz und weiterer in diesem Zusammenhang relevanter Rechtsnormen, die sich für den Auftraggeber als Verantwortlicher für die Datenverarbeitung und den Auftragnehmer als Auftragsverarbeiter ergeben.

Im Falle von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

2. Verantwortlichkeit

Es gelten die festgelegten Verantwortlichkeiten aus Kapitel 18.1

Die Inhalte dieses AV-Vertrages gelten bei Datenverarbeitungen, auch wenn Prüfungen oder Wartungen automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen werden und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie, bzgl. des Datenschutzes, einschlägigen Rechtsnormen verantwortlich.

3. Dauer des Auftrags

Der Vertragsbeginn dieses Vertrages, seine Laufzeit sowie die Kündigungsfristen entsprechen den in Kapitel 18.2 getroffenen Festlegungen.

Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen Auftragsverarbeitungsvertrags, z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

4. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten des Auftraggebers erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers.

Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen, sofern dies nicht gesetzlich untersagt ist. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

Die Weisungen des Auftraggebers werden vom Auftraggeber dokumentiert und dem Auftragnehmer unmittelbar nach erfolgter Dokumentation schriftlich oder in Textform zur Verfügung gestellt.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bzgl. des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

Es kann gerade vorkommen, dass eine schnelle Reaktion des Auftragnehmers erforderlich ist, welche eine vorherige schriftliche Beauftragung nicht ermöglicht. Reagiert der Auftragnehmer hier auf eine mündliche Beauftragung seitens des Auftraggebers, um Schaden von Betroffenen abzuwenden, so muss der Auftraggeber eine schriftliche Beauftragung nachreichen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in Textform bestätigen.

5. Leistungsort

Der Auftragnehmer und etwaige Unterauftragnehmer werden die vertraglichen Leistungen am Ort der in Kapitel 18.5 getroffenen Festlegung erbringen.

Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden Rechtsnormen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittland“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

Erfolgt eine Leistungserbringung durch den Auftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen datenschutzrechtlichen Vorgaben und weist dies auf Verlangen nach. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer.

Bei einer Leistungserbringung in einem sicheren Drittland wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen datenschutzrechtlichen Vorgaben wird durch den Auftragnehmer gewährleistet.

Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z.B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

Sofern die Datenverarbeitung nach dieser Vereinbarung und den gültigen Rechtsnormen zur Verarbeitung personenbezogener Daten im Auftrag außerhalb Deutschlands erbracht werden darf, bzw. die Übermittlung personenbezogener Daten in das Ausland zulässig ist, wird der Auftragnehmer für die Einhaltung und Umsetzung der normativen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

6. Pflichten des Auftragnehmers

Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus den gültigen Rechtsnormen resultierenden Maßnahmen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Kapitel 1 zu diesem Vertrag.

Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen, Privatgeheimnissen und Datensicherheitsmaßnahmen des Verantwortlichen oder der Auftraggeber vertraulich zu behandeln. Der Auftragnehmer gewährleistet, dass alle Personen, welche im Rahmen der Auftragsverarbeitung tätig sind, zusätzlich zur Wahrung des Datengeheimnisses, zur Wahrung des Fernmeldegeheimnisses, zur Wahrung von Geschäfts- und Betriebsgeheimnisse und zur Wahrung von Privatgeheimnissen nach dem jeweils gültigen Recht, wie in Kapitel 19 angegeben, verpflichtet sind.

Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit die in Kapitel 18.6 angegebene Person benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

Ist der Auftraggeber aufgrund geltender Rechtsnormen gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt, sofern die Auftragsverarbeitung oder die Daten des Auftraggebers von den Kontrollen oder Maßnahmen betroffen sind oder Gegenstand der Maßnahmen oder Kontrollen sind.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen Rechtsnormen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem

Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der für den Datenschutz gültigen Rechtsnorm liegen.

Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden.

Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

Beinhaltet die beauftragte Verarbeitung Daten die dem Privatgeheimnis nach 203 StGB unterliegen, gelten die Vereinbarungen aus Anlage 2.

Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

7. Fernzugriff auf Systeme des Auftraggebers bei Prüfung/Wartung oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend die in Kapitel 18.8 getroffenen Vereinbarungen zu den Rechten und Pflichten des Auftraggebers und Auftragnehmers:

8. Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist der Verantwortliche zuständig. Der Auftraggeber oder Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die sich aus den gültigen Rechtsnormen ergebenden Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann. Dies gilt auch für den Fall, wenn der Auftragnehmer mit dem Auftraggeber vereinbart, dass die Leistungen zugunsten Dritter, so wie in Kapitel 18.10.4 benannt, erbracht werden.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

Dem Auftraggeber obliegen bzgl. des Datenschutzes die aus den jeweilig gültigen Rechtsnormen resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von der Verarbeitung der personenbezogener Daten Betroffenen.

Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

Weiterhin sind alle Personen des Auftraggebers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftragnehmers zu verpflichten und müssen auf jeweils gültige Rechtsnormen hingewiesen werden.

Der Auftraggeber stellt sicher, dass die aus den bzgl. des Datenschutzes gültigen Rechtsnormen resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

9. Kontrollrechte des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichende Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der gültigen Rechtsnormen erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Hierfür kann er beispielsweise Selbstauskünfte, Zertifikate und Prüfberichte beim Auftragnehmer einholen oder sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere der Einhaltung und ggf. notwendigen Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags, wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

10. Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Haupt-Vertrag bereits eine entsprechende Regelung getroffen worden ist.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

Nach Abschluss der vertraglichen Arbeiten - oder früher nach Aufforderung durch den Auftraggeber - hat der Auftragnehmer sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger, erstellte Verarbeitungsergebnisse, Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostenübernahme.

Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.

Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag anders vereinbart. In besonderen, vom Auftraggeber zu bestimmenden, Fällen erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

11. Unterauftragnehmer

Für die Beauftragung von Unterauftragnehmern gelten die in Kapitel 18.10 getroffenen Vereinbarungen. Wird dem Auftragnehmer die Beauftragung von weiteren Unterauftragnehmern gestattet, gelten die folgenden zusätzlichen Vereinbarungen.

Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragnehmer durch Unterauftragnehmer des Auftragnehmers beauftragt werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.

Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Kapitel 18.10 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien

dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

Eine zustimmungspflichtige Unterbeauftragung liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen. Je nach Hauptleistung wird die Nebenleistung in Kapitel 18.10.3 festgelegt,

Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

12. Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

13. Haftung

Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht den gültigen Rechtsnormen entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

- er den aus den gültigen Rechtsnormen resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
- er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

- seinen ihm speziell durch die gültigen Rechtsnormen auferlegten Pflichten nicht nachgekommen ist oder

- unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

Weitergehende Haftungsansprüche nach den allgemeinen Rechtsnormen bleiben unberührt.

14. Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

15. Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge von Änderungen der Rechtsnormen nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

16. Rechtswahl, Gerichtsstand

Es gilt: ☐ Deutsches Recht

Gerichtsstand ist der Sitz des Auftraggebers.

Auftragnehmer

Ort, Datum

Auftraggeber

Ort, Datum

Klaus Fritsch
Geschäftsführer
Nexus digital pathology GmbH

Andreas Giebisch
Geschäftsführer
Nexus digital pathology GmbH

Arnd Liman
Geschäftsführer
Nexus digital pathology GmbH

Michael Schaaf
Geschäftsführer
Nexus digital pathology GmbH

Anlage 1

Diese Anlage ist Bestandteil der standardisierten Vertragsvorlage für Auftragsverarbeitungsverträge der Nexus Unternehmensgruppe. Sie bezieht sich auf die **unveränderte** Version dieses Auftragsverabeitungsvertrages für D- EU/ EWR

☒ Ja ☐ Nein

Nexus Auftragsverarbeitungsvertrag im Unternehmensverbund

Nexus Auftragsverarbeitungsvertrag im Unternehmensverbund
☐ Ja

☒ Die Leistungen sind in Kapitel 17.1 beschrieben

17. Hauptvertrag

17.1. Leistungen

☐ Zwischen Auftraggeber und Auftragnehmer besteht ein gültiger Hauptvertrag/ Leistungsvertrag oder sonstiger Vertrag. Der Vertrag beschreibt die zu erbringenden Leistungen.

☐ Vertragsname:_____

☐ Datum:_____

☐ Vertragsnummer:_____

☐ Vertragsanlagen:_____

☐ Es besteht kein gültiger Hauptvertrag/ Leistungsvertrag oder sonstiger Vertrag zwischen den Vertragsparteien. Der Auftragnehmer erbringt für den Auftraggeber die im Folgenden beschriebenen Leistungen.

- Leistungsschein
- Leistung
- Leistung

18. Auftragsverarbeitungsvertrag

18.1. Verantwortlichkeit

☐ Der Auftraggeber ist der für die Verarbeitung Verantwortliche, er ist im Rahmen dieses Vertrages selbst für die Einhaltung der Rechtsnormen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

☐ Der im vorliegenden Vertrag als Auftraggeber bezeichnete, ist für die vorliegende Verarbeitung selbst als Auftragnehmer eines dritten oder des Verantwortlichen tätig. Die Verantwortung für die Rechtmäßigkeit der Verarbeitung liegt in diesem Fall beim für die Verarbeitung Verantwortlichen.

18.2. Laufzeit des Auftragsverarbeitungsvertrages

☐ Dieser Vertrag ersetzt den bereits bestehenden Auftragsverarbeitungsvertrag vom [Datum]

☒ Der Vertrag beginnt ab dem [Datum]

☐ und läuft bis zum [Datum] (Mindestvertragslaufzeit).

☒ und hat keine vorgegebene Vertragslaufzeit.

☐ Der Vertrag kann danach seitens des Auftraggebers mit einer Frist von [Anzahl der Monate] Monaten zum Ende der Vertragslaufzeit gekündigt werden, ansonsten verlängert er sich um ein weiteres Jahr.

☐ Der Vertrag kann danach seitens des Auftragnehmers mit einer Frist von [Anzahl der Monate] Monaten zum Ende der Vertragslaufzeit gekündigt werden, ansonsten verlängert er sich um weitere [Anzahl der Monate] Monate.

☒ Die Laufzeit des Vertrages entspricht der im Hauptvertrag festgelegten Laufzeit.

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

18.3. Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind:

☒ Geschäftsführung

☒ Teamleitung [TEAM]

☐ IT-Leitung

☐ Systembetreuer

☐ Ärzte

☐ Pflegekräfte, Arzthelferinnen

☐ Sachbearbeiter [Sachgebiet]

☐ Weitere vom Auftraggeber mit der Betreuung der Daten des Auftraggebers beauftragte Personen [Position oder Funktion oder Vorname, Nachname]

18.4. Weisungsempfänger beim Auftragnehmer sind:

☒ Geschäftsführung

☒ Teamleitung [TEAM]

☐ IT-Leitung

☐ Systembetreuer

☐ Ärzte

☐ Pflegekräfte, Arzthelferinnen

☐ Personalsachbearbeiter

☐ Weitere vom Auftragnehmer mit der Betreuung der Daten des Auftraggebers beauftragte Personen [Position oder Funktion oder Vorname, Nachname]

18.5. Ort der vertraglichen Leistungserbringung

Der Auftragnehmer wird die vertraglichen Leistungen

x in Deutschland erbringen.

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen.

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen.

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder im Drittland Schweiz erbringen

Etwaige Unterauftragnehmer werden die sie betreffenden Leistungen

x in Deutschland erbringen.

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen.

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen.

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder im Drittland Schweiz

18.6. Datenschutzbeauftragter des Auftragnehmers

Name Daniel Schropp

E-Mailadresse datenschutz@nexus-ag.de

☐ Der Auftragnehmer ist Einzelunternehmer oder unterliegt nicht der Pflicht, einen Datenschutzbeauftragten zu benennen.

18.7. Datenschutzbeauftragter des Auftraggebers

Name

E-Mailadresse

☐ Der Auftraggeber ist Einzelunternehmer oder unterliegt nicht der Pflicht, einen Datenschutzbeauftragten zu benennen.

18.8. Fernzugriff auf Systeme des Auftraggebers

☐ Es wird nicht per Fernzugriff auf das System/die Systeme des Auftraggebers zugegriffen

☒ Es wird per Fernzugriff auf das System/die Systeme des Auftraggebers zugegriffen

Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen. Es werden angemessene Identifizierungs- und Verschlüsselungsverfahren eingesetzt.

Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.

Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach ihrer Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom

verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder anderem verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichermedien oder ähnliche Geräte) kopiert werden.

Der Auftraggeber und der Auftragnehmer vereinbaren ein angemessenes Verfahren zur Beauftragung und Freigabe von Fernzugriffen oder eines Datenabzuges.

18.9. Datenarten, Zwecke der Verarbeitung und Kreis der Betroffenen

18.9.1. Art der Daten

☒ **Personalstamm- und Bewegungsdaten**

wie z. B. Personalnummer, Vorname, Anschrift, Telefonnummer, E-Mail-Adresse,

☒ **Bewohner-/ Klienten-/ Patientendaten**

wie z. B. Geschlecht, Vorname, Nachname, Anschrift, Telefonnummer, E-Mail-Adresse, Geburtsdatum, -ort, Kundennummer, Konfession, Familienstand, Nationalität, …

☐ **Vertragsstamm, Abrechnungs-, Zahlungs- und Bewegungsdaten**

wie z. B. Bankverbindung, Allgemeine biografische Daten

☒ **Kundendaten, Kundenhistorie**

wie z. B. Geschlecht, Vorname, Nachname, Anschrift, Telefonnummer, E-Mail-Adresse,

☐ **Auskunftsangaben**

wie z.B. von Dritten, wie Auskunfteien, oder aus öffentlichen Verzeichnissen

☐ **Daten von Kostenträgern, Ämtern, Institutionen und Organisationen**

wie z. B. Anschrift, Ansprechpartner, Bankverbindung, Pflegesätze, Verwahrungsgelder

☒ **Daten von Lieferanten**

wie z. B. Bezeichnung, Anschrift, Telefonnummer, Ansprechpartner, Bankverbindung, …

☐ **Termin-, Planungs- und Steuerungsdaten**

wie z.B. Reiseverlauf

☐ **Sozialdaten**

wie z. B. Sozialversicherungsnummer

☐ **Genetische, biometrische Daten**

wie z. B. Fingerabdruck, Lichtbild, Unterschrift, …

☐ **Gesundheitsdaten**

wie z. B. Behinderungsgrad, Krankheiten, …

☒ **Medizinische Patientendaten**

wie z. B. Krankheitsbilder, Diagnosen, Pflegestufe, Rezepte, Einstufung in DRG, …

☐ **Weitere** ……

☐ **Weitere** ……

18.9.2. Zweck der Datenverarbeitung

☒ Systemwartung, Problemanalyse und –behebung auf dem System des Auftraggebers

☒ Projektbetreuung bei Umsetzung von Customizing-Aufträgen und von Implementierungsaufträgen auf dem System des Auftraggebers

☐ Lohn- und Gehaltsabrechnung

☐ Elektronische Personalakte (perspektivisch)

☐ Dienstplan / Software zur elektronischen Dienst- und Fortbildungsplanung

☐ Controlling

☐ Faktura, Abrechnung der Heimentgelte

☐ Customer Relationship Management

☐ Planung von pflegerischen, ärztlichen und therapeutischen Maßnahmen

☐ Elektronische Pflegedokumentation

☐ Allgemeiner Einkauf

☐ Bewohner-/ Klienten-/ Patientenversorgung

☐ Fuhrparkverwaltung

☐ Betrieb des Einkaufsportals

☐ Rechnungsstellung/ -begleichung

☐ Dokumentenmanagementsystem

☐ Inventarisierung

☐ Lager- und Bestandsverwaltung

☐ Bewerbermanagement

☐ Marketing

☐ Weitere ……..……..

☐ Weitere ……..……..

18.9.3. Kreis der Betroffenen

☒ Beschäftigte, Mitarbeiter

☐ Ehemalige Beschäftigte, Mitarbeiter

☐ Bewerber

☒ Kunden

☒ Kunden von Kunden

☐ Zeitarbeiter

☒ Bewohner von Pflegeheimen / Klienten / Patienten

☐ Ehemalige Bewohner von Pflegeheimen / Klienten / Patienten

☐ Alle Kostenträger, Ämter, Institutionen und Organisationen,

wie z. B. Krankenkassen, Pflegekassen, Sozialämtern, Finanzämter, Förderungen, Agentur für Arbeit

☐ Lieferanten und Dienstleister

☐ Weitere ……..……..

☐ Weitere ……..……..

18.10. Unterauftragnehmer

☐ Die Beauftragung von Unterauftragnehmern ist dem Auftragnehmer nicht erlaubt. Eine Weitergabe von Aufträgen vereinbarter Tätigkeiten an Unterauftragnehmer durch den Auftragnehmer erfolgt nicht.

☐ Die Beauftragung von Unterauftragnehmern ist dem Auftragnehmer erlaubt. Es wird hiermit durch den Auftraggeber eine Genehmigung für Beauftragungen von Unterauftragnehmern aus der Unternehmensgruppe nach Kapitel 18.10.1 erteilt. Weitere Beauftragungen von Unterauftragnehmer bedürfen einer expliziten Genehmigung durch den Auftraggeber.

☐ Die Beauftragung von Unterauftragnehmern ist dem Auftragnehmer erlaubt. Es wird hiermit durch den Auftraggeber eine Genehmigung für Beauftragungen von Unterauftragnehmern aus der Unternehmensgruppe nach Kapitel 18.10.1, sowie weiteren Unterauftragnehmern nach 18.10.2 erteilt. Weitere Beauftragungen von Unterauftragnehmern bedürfen einer expliziten Genehmigung durch den Auftraggeber.

☐ Die Beauftragung von Unterauftragnehmern ist dem Auftragnehmer erlaubt. Die Erlaubnis zur Beauftragung der Unterauftragnehmer aus den Kapiteln 18.10.1 und 18.10.2 wird erteilt. Es wird hiermit durch den Auftraggeber dem Auftragnehmer eine allgemeine Genehmigung für die Beauftragung von weiteren Unterauftragnehmern erteilt. Der Auftraggeber behält sich vor, die allgemeine schriftliche Genehmigung zu widerrufen bzw. zu beschränken. In diesem Fall dürfen weitere Unterauftragnehmer nur noch bei expliziter schriftlicher Genehmigung hinzugezogen werden.

18.10.1. Verbunde Unternehmen des Auftragnehmers

☐ Keine Unterauftragnehmer

Der Auftragnehmer befindet sich in einer Unternehmensgruppe. Die Leistungen der Auftragsverarbeitung werden beim Auftragnehmer, ganz oder teilweise, durch verbundene Unternehmen aus der Unternehmensgruppe des Auftragnehmers erbracht.

Vom Auftragnehmer benannte und vom Auftraggeber genehmigte Unterauftragnehmer:

Name und Anschrift des Unternehmens	Beschreibung der Teilleistungen Ort der Leistungserbringung
Nexus Cloud IT GmbH, Irmastraße 1, 78166 Donaueschingen	Server Hosting

Name und Anschrift des Unternehmens	Beschreibung der Teilleistungen Ort der Leistungserbringung

18.10.2. Sonstige Unterauftragnehmer des Auftragnehmers

x Keine Unterauftragnehmer

Sonstige Unterauftragnehmer sind alle Unterauftragnehmer die nicht zum Unternehmensverbund der NEXUS Unternehmensgruppe gehören und keine Nebenleitungen erbringen.

Name und Anschrift des Untervertragsnehmer	Beschreibung der Teilleistungen Ort der Leistungserbringung
…	…

Name und Anschrift des Untervertragsnehmer	Beschreibung der Teilleistungen Ort der Leistungserbringung

18.10.3. Unterauftragnehmer beim Auftragnehmer für Nebendienstleistungen

xIB Keine Nebendienstleister

Eine zustimmungspflichtige Beauftragung von Unterauftragnehmern liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt. Nebenleistungen sind ausschließlich:

Nebenleistungen	Name Anschrift

18.10.4. Verbundene Unternehmen des Auftraggebers

Der Auftraggeber befindet sich in einer Unternehmensgruppe. Die Auftragsverarbeitung wird vom Auftragnehmer ganz oder teilweise für Unternehmen aus der Unternehmensgruppe des Auftraggebers erbracht. Dies sind Leistungen zugunsten Dritter. Solche Dritte und die für sie erbrachten Leistungen, werden im Folgenden benannt.

Name und Anschrift des Unternehmens (Dritten)	Beschreibung der Teilleistungen Ort der Leistungserbringung
…	

19. Gültige Rechtsnormen

Für diesen Vertrag und die damit verbundene Verarbeitung von personenbezogenen Daten sind die folgenden Rechtsnormen zu beachten.

19.1. Europa und europäischer Wirtschaftsraum (EU/ EWR)

☒ EU – DSGVO - Europäische Datenschutz Grundverordnung

19.2. Deutschland

☒ BDSG - Bundesdatenschutzgesetz

☒ Landesdatenschutzgesetz des Landes in dem der Auftraggeber seinen Hauptsitz der Unternehmung hat.

☐ Landeskrankenhausgesetz des Landes in dem der Auftraggeber seinen Hauptsitz der Unternehmung hat.

☐ Kirchlicher Datenschutz

☐ DSG-EKD - Datenschutzgesetz der evangelischen Kirche in Deutschland
Siehe auch Zusatzvereinbarung zum kirchlichen Datenschutz Kapitel 22

☐KDG - Datenschutzgesetz der römisch-katholischen Kirche in Deutschland
Siehe auch Zusatzvereinbarung zum kirchlichen Datenschutz Kapitel 23

☐ StGB – Strafgesetzbuch
Im Besonderen
§ 203 - Verletzung von Privatgeheimnissen (siehe auch Kapitel 6)
....

☒ GeschGehG - Gesetz zum Schutz von Geschäftsgeheimnissen
Im Besonderen
§ 23 - Verletzung von Geschäftsgeheimnissen

☐ TKG – Telekommunikationsgesetz
Im Besonderen
§ 88 – Fernmeldegeheimnis

Weitere Rechtsnormen
☐ _____
☐ _____

20. Technische und organisatorische Maßnahmen

Die getroffenen Maßnahmen bitte ausführlich beschreiben. Ggf. sind weiterführende Dokumentationen bitte anzufügen.

Bitte Beschreiben sie kurz das Verfahren/ IT-Sytem zur betroffenen Datenverarbeitung.

IBSv3 mit den zusätzlichen Modulen Theben und order-entry. Es werden Befunde und Aufträge digital übermittelt.

20.1. Zutrittskontrolle

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass ein unbefugter Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verhindert wird?

☐ Keine Relevanz für die Art der Datenverarbeitung

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch elektronische Schlüssel, Alarmanlagen, Videoanlagen;

20.2. Zugangskontrolle

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass ein unbefugter Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verhindert wird?

☐ Keine Relevanz für die Art der Datenverarbeitung

Keine unbefugte Systembenutzung, durch sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

20.3. Zugriffskontrolle

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass ein unbefugter Zugriff auf Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verhindert wird?

☐ Keine Relevanz für die Art der Datenverarbeitung

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen Die Systemkomponenten des Auftragnehmers werden dem Auftraggeber in einer virtuellen Maschine (Linux-VM) zum Herunterladen von der hompage des Auftragnehmers angeboten und sind mittels eines individuellen Initialisierungs-Codes aktivierbar. Der direkte Zugriff auf die virtuelle Maschine des Auftragnehmers ist vor Fremdeinwirkung geschützt und nur dem Auftragnehmer vorbehalten.

20.4. Integrität

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden?

☐ Keine Relevanz für die Art der Datenverarbeitung

Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur; Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in interne Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden durch Protokollierung, Dokumentenmanagement; externe Feststellung ist nicht erforderlich, da nur automatisierte und keine manuellen Prozesse die Eingabe steuern und im Verantwortungsbereich des Auftraggebers liegen

20.5. Verfügbarkeit/ Wiederherstellung

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird,

- dass personenbezogene Daten nicht zufällig verändert oder zerstört werden oder verloren gehen?
- dass alle IT-Systeme zur Verfügung stehen?
- dass Vorfälle/ Fehfunktionen gemeldet werden?
- dass IT-Systeme im Störungsfall wiederhergestellt werden können?

☐ Keine Relevanz für die Art der Datenverarbeitung

Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch BackupStrategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

20.6. Belastbarkeit

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass IT-Systeme belastbar sind?

☐ Keine Relevanz für die Art der Datenverarbeitung

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) redundante Virtualisierung, Ersatzteil Vorhaltung, Loadbalancing

20.7. Pseudonymisierung/ Anonymisierung

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass Daten so verarbeitet werden, dass pseudonymisierte Daten ohne zusätzliche

Informationen nicht mehr einer identifizierbaren Person zugeordnet werden können oder dass personenbezogene Daten anonymisiert werden, wenn dies möglich ist?

☒ Keine Relevanz für die Art der Datenverarbeitung

20.8. Transportkontrolle/ Übertragungskontrolle/ Weitergabekontrolle

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird,

- dass bei der Übertragung personenbezogener Daten, sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten nicht verletzt wird?
- dass gespeicherte personenbezogene Daten oder personenbezogene Daten bei der Übertragung durch Verschlüsselungsmaßnahmen geschützt werden?
- dass personenbezogene Daten nicht bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☐ Keine Relevanz für die Art der Datenverarbeitung

Datenschutz-Management Zutrittsperre für Unbefugte, Schutz vor unbefugter Einsicht, Vergitterter Serverraum mit elektronischem Zutrittschutz, Alarmanlage mit Bewegungsmelder, Fenster- und Türkontakten Incident-Response-Management standortübergreifende, redundante, multi-OS-verteilte Virtualisierung Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) Übertragung erfolgt Ende-Zu-Ende verschlüsst, Einblick in personenbezogene Daten durch Nexus Personal erfolgt nur nach fallbezogener Aufforderung des Auftraggebers

20.9. Regelmäßige Überprüfungen

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass die Wirksamkeit der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüft, bewertet und evaluiert werden?

☐ Keine Relevanz für die Art der Datenverarbeitung

Regelmäßige interne Überprüfungen im Rahmen des DSMS

20.10.Auftragskontrolle

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass personenbezogene Daten, nur nach Weisung des Verantwortlichen/ des Auftraggebers verarbeitet werden?

☐ Keine Relevanz für die Art der Datenverarbeitung

Fernwartung auf Kundensystemen wird ausschließlich in dem Umfang durchgeführt, wie sie vertraglich festgelegt sind.

Mitarbeiter, die Fernwartung auf Kundensystemen durchführen, haben Kenntnis über den vertraglich festgelegten Rahmen und kennen die weisungsbefugten Personen der Auftraggeber.

20.11. Datenportabilität

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass von Betroffenen selbst zur Verfügung gestellte personenbezogene Daten, in einem strukturierten, gängigen und maschinenlesbaren Format, diesem oder an die verantwortliche Stelle/ den Auftraggeber übermittelt werden können?

☐ Keine Relevanz für die Art der Datenverarbeitung

Die vom Betroffenen selbst zur Verfügung gestellten Daten, welche durch den Auftraggeber gespeichert wurden, können auf Anforderung in einem strukturierten, gängigen und maschinenlesbaren Format an den Betroffenen herausgegeben werden. Dies gilt auch für die Übermittlung an eine andere verantwortliche Stelle.

20.12.Trennbarkeit

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird,

- dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden?
- dass personenbezogene Daten unterschiedlicher verantwortlicher Stellen/ Auftraggeber getrennt verarbeitet werden können?

☐ Keine Relevanz für die Art der Datenverarbeitung

Die zu unterschiedlichen Zwecken erhobenen Datenbestände sind voneinander getrennt.

Die Datenfelder können je unterschiedlichem Zweck voneinander unabhängig verarbeitet werden (bspw. Löschung).

20.13.Löschbarkeit

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird,

- dass mit Zweckerfüllung, bzw. Ablauf der Aufbewahrungspflicht personenbezogene Daten datenschutzkonform gelöscht werden?

- dass der Betroffene sein Recht auf Löschung seiner personenbezogenen Daten wahrnehmen kann?

☐ Keine Relevanz für die Art der Datenverarbeitung

Löschungen sind nach Auftrag jederzeit möglich

20.14.Auskunft an Betroffene

Welche techn./organisatorischen Maßnahmen werden umgesetzt, damit gewährleistet wird, dass der Betroffene sein Recht auf Auskunft über die über ihn gespeicherten personenbezogenen Daten wahrnehmen kann?

☐ Keine Relevanz für die Art der Datenverarbeitung

Ist nach Auftrag jederzeit möglich

Auftragnehmer

_____

Ort, Datum

_____

Vorname Nachname

Position

Firmenname

Anlage 2
21. Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203 und 204 StGB (D)

Wenn der Auftragsverarbeiter als Dienstleister an Tätigkeiten von Berufsgeheimnisträgern mitwirkt, die einer beruflichen Verschwiegenheitsverpflichtung unterliegen, gilt folgendes:

Der Auftragnehmer und alle Personen die im Zusammenhang mit der Beauftragung für den Auftraggeber tätig sind, unterliegen, wie der Berufsgeheimnisträger, einer Verschwiegenheitspflicht und haben ebenso ein Zeugnisverweigerungsrecht. Informationen die beim Auftraggeber dem Beschlagnahmeschutz unterliegen, unterliegen auch beim Auftragnehmer dem Beschlagnahmeschutz. Der Auftragsverarbeiter und insbesondere die Beschäftigten des Auftragsverarbeiters, wahren daher, in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht fremde Geheimnisse, die ihnen zugänglich gemachten werden.

Der Auftragnehmer ist verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Der Auftragnehmer hat seine Mitarbeiter, soweit sie in Erfüllung dieser Vereinbarung für den Auftraggeber tätig werden, zur Verschwiegenheit zu verpflichten, auf das Zeugnisverweigerungsrecht und Beschlagnahmeverbot sowie auf die strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht hinzuweisen. Die Pflicht zur Verschwiegenheit besteht auch nach Beendigung des Verhältnisses zeitlich unbegrenzt fort.

Ist dem Auftragsverarbeiter erlaubt, weitere Personen (Dritte) zur Erfüllung des Vertrages heranzuziehen, so gilt obiges ebenso für diese. Daher sind diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese Dritten im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen erlangen könnten. Die Verpflichtung erfolgt durch den Dritten und wird auf Verlangen dem Auftragsverarbeiter zur Verfügung gestellt.

Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Auftragnehmer aufgrund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragnehmer den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

Anlage 3
22. Zusatzvereinbarung evangelisches Datenschutzgesetz (EKD) (D)

In Ergänzung des zwischen den Parteien geschlossenen Vertrages zur Auftragsverarbeitung nach Art. 28 DSGVO kommen Auftraggeber und Auftragnehmer überein, dass für die Auftragsdatenverarbeitung nach dieser Vereinbarung auch der kirchliche Datenschutz der evangelischen Kirche in Deutschland (EKD) Anwendung findet.

Der Auftraggeber verpflichtet sich zusätzlich gemäß § 30 Abs. 5 Satz 3 EDG, sich der kirchlichen Datenschutzaufsicht zu unterwerfen. Die Unterwerfung erstreckt sich auch auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD.

Anlage 3
23. Zusatzvereinbarung katholisches Datenschutzgesetz (KDG) (D)

In Ergänzung des zwischen den Parteien geschlossenen Vertrages zur Auftragsverarbeitung nach Art. 28 DSGVO kommen Auftraggeber und Auftragnehmer überein, dass für die Auftragsdatenverarbeitung, nach dieser Vereinbarung, auch der kirchliche Datenschutz der katholischen Kirche in Deutschland (KDG) Anwendung findet.

Der Auftraggeber verpflichtet sich zusätzlich gemäß § 29, §30 KDG, sich der kirchlichen Datenschutzaufsicht zu unterwerfen. Dies erstreckt sich auch auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach § 42 Abs. 1 KDG.