Vereinbarung zur Verarbeitung von Daten im Auftrag gem. Art. 28 DSGVO

- dem Auftraggeber, nachstehend auch „Verantwortlicher“ genannt und
- dem Konsortium „Pre-Screening-Tool für klinische Studien"
- w7 GmbH Adresse: Rhönstr. 89, 63571 Gelnhausen vertreten durch: David Mann
- und
- Patient-Health-Innovation GmbH Adresse: Berlinickestr.2, 12165 Berlin vertreten durch: Dr. Michael Kretschmann und Nicole Wolters-Hildebrandt

1. Gegenstand und Dauer des Auftrags

1.1 Der Gegenstand des Auftrags und seine Dauer ergeben sich aus dem Vertrag über die Bereitstellung des Online-Dienstes ,,Pre-Screening Tool“ einschließlich der hierzu vereinbarten Nutzungsbedingungen und etwaiger Zusatzvereinbarungen.

1.2 Die Dauer der Datenverarbeitung ergibt sich aus dem oben genannten Vertrag und aus eventuell geschlossenen Zusatzvereinbarungen.

1.3 Die Vorgaben dieser Vereinbarung wirken nach, so lange der Auftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeitet.

2. Konkretisierung des Auftragsinhalts

2.1 Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den

Auftragsverarbeiter für den Verantwortlichen lassen sich wie folgt beschreiben: Bereitstellung (inkl. Hosting), Betrieb, Wartung und Weiterentwicklung der webbasierten Software „Pre-Screening Tool“. Die Software dient der Vorselektion von Patienten für klinische Studien. Die Verarbeitung erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen gegenüber den Verantwortlichen sowie nach dessen Weisung.

2.2 Die Arten der verarbeiteten personenbezogenen Daten sowie die Kategorien der betroffenen Personen umfassen insbesondere:

a) Kategorien personenbezogener Daten

- Stammdaten von Teilnehmenden, z.B. Patienten und Angehörige
- Kontaktdaten
  (z. B. E-Mail-Adresse, Telefonnummern, Kontaktdaten von Angehörigen)
  Kommunikationsdaten
  (z. B. Nachrichten, Mitteilungen, Terminabsprachen, interne Vermerke)
- Technische Nutzungsdaten
  (z. B. Logdaten, Zeitpunkte von Zugriffen, IP-Adressen, Protokolle von Aktivitäten im System)
- Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO
  soweit durch den Verantwortlichen im System verarbeitet, insbesondere Gesundheitsdaten
  (z. B. Angaben zu Vorerkrankungen, Begleitmedikationen, etc.

Darüber hinaus können personenbezogene Daten verarbeitet werden, die vom Verantwortlichen oder von Nutzern eigenständig in das System eingegeben oder hochgeladen werden.

b) Kategorien betroffener Personen

- Patienten
- Angehörige
- Nutzer (Ärzte/ Studienkoordinatoren) der Software

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter ergreift in seinem Verantwortungsbereich alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten und übergibt dem Verantwortlichen die Dokumentation zur Prüfung (Anlage 2.a). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage der Vereinbarung.

3.2 Soweit eine Prüfung oder ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3 Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragsverarbeiter zu dokumentieren sind, ist der Verantwortliche in Kenntnis zu setzen.

4. Rechte von betroffenen Personen

4.1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von betroffenen Personen erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

4.2 Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß Nr. 4 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

5. Qualitätssicherung und sonstige Pflichten

Der Auftragsverarbeiter hat (zusätzlich zu den Pflichten nach dieser Vereinbarung) eigene gesetzliche Pflichten gemäß der DSGVO. Hierzu zählen insbesondere, aber nicht nur:

1. Der Auftragsverarbeiter bestellt – soweit gesetzlich erforderlich – schriftlich einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und Art. 39 DSGVO ausübt.
2. Der Auftragsverarbeiter wahrt die Vertraulichkeit gemäß Art. 28 Abs. 3 Buchst. b, Art. 29, Art. 32 Abs. 4 DSGVO. Deshalb setzt er bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Er und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, es besteht eine gesetzliche Verpflichtung zur Datenverarbeitung.
3. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
4. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
5. Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
6. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten, die sich aus den Artikeln 32 bis 36 DSGVO ergeben.
7. Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
8. Der Auftragsverarbeiter kann die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Nr. 8 dieser Vereinbarung nachweisen.
9. Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Verantwortlichen in der Weise, dass der Verantwortliche seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Verantwortlichen für weitere Maßnahmen zur Verfügung stellt.

10. Der Auftragsverarbeiter unterstützt den Verantwortlichen in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
11. Soweit der Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragsverarbeiter nach diesem Vertrag stehen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Verantwortlichen beauftragen. Der Verantwortliche stimmt der Beauftragung der in Anlage 2.b bezeichneten Unterauftragnehmer zu.
   Die Auslagerung auf Unterauftragnehmer und der Wechsel von bestehenden Unterauftragnehmern sind nur zulässig, soweit
   a) der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragnehmer dem Verantwortlichen eine angemessene Zeit vorab (mindestens 14 Tage) schriftlich oder in Textform anzeigt und
   b) der Verantwortliche bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter nicht schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
   c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO sowie die Vorgaben dieser Vereinbarung zugrunde gelegt werden. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend dieser Vereinbarung und gemäß der Datenschutz-Grundverordnung unterliegt.

6.3 Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter die betreffenden Passagen der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

6.4 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

7. Internationale Datenübermittlungen

7.1 Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Datenschutz-Grundverordnung im Einklang stehen.

7.2 Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Nr. 6 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten in Drittländer beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Datenschutz-Grundverordnung sicherstellen.

8. Kontrollrechte des Auftraggebers

8.1 Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das

Recht, sich selbst oder durch einen beauftragten Dritten durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

8.2 Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Weisungsbefugnis des Auftraggebers

9.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Datenschutz-Grundverordnung oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung auszusetzen, bis der Verantwortliche die Weisung geändert hat oder diese bestätigt.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen auf Wunsch, dass dies erfolgt ist, oder gibt dem Verantwortlichen diese Daten in einem vereinbarten Format zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung fortbesteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Vereinbarung.

11. Weitere Regelung

Im Fall eines Widerspruchs zwischen dieser Vereinbarung zur Verarbeitung von Daten im Auftrag und anderer Vereinbarungen zwischen den Parteien hat diese Vereinbarung Vorrang.

Anlage 2.a: Technische und organisatorische Maßnahmen des Auftragnehmers

nach Art. 32 DSGVO
zu Nr. 3 der Anlage 2 (Auftragsverarbeitung)

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

1.1 Zutrittskontrolle
Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.
- Die Verarbeitung personenbezogener Daten erfolgt in Rechenzentren externer Hosting-Dienstleister
- Physische Zutrittskontrollen werden durch die eingesetzten Subdienstleister (z. B. Cloud-Anbieter) sichergestellt
- Der Auftragsverarbeiter hat keinen eigenen physischen Zugriff auf die Serverinfrastruktur
- Zugriff auf Büro- und Arbeitsumgebungen erfolgt nur für berechtigte Personen

1.2 Zugangskontrolle
Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern.
- Systeme sind nur nach einem individuellen Login nutzbar
- Login mit Kennwortverfahren (mit Vorgaben für komplexe Kennwörter)
- Einsatz von Multi-Faktor-Authentifizierung (MFA), soweit möglich
- Einrichtung eines Benutzerstammsatzes pro User
- automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware
- Verschlüsselung von gespeicherten Daten nach dem Stand der Technik (z. B. AES-256 bei Cloud-Speicherung)

1.3 Zugriffskontrolle
Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.
- Zugriff auf Systeme nur nach individuellem Login
- Login mit Kennwortverfahren (komplexe Kennwörter)
- differenzierte Berechtigungen (z. B. Rollenmodelle für Administratoren, Nutzer, Support)
- Zugriffe auf Anwendungen und/oder Daten werden protokolliert und können ausgewertet werden
- Anzahl der administrativen Zugriffe wird auf ein notwendiges Minimum reduziert
- Zugriff auf personenbezogene Daten erfolgt ausschließlich nach dem Need-to-know-Prinzip, einstellbar in den Einstellungen der Software
- administrative und Support-Zugriffe sind auf berechtigte Personen beschränkt

1.4 Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.
- interne Mandantenfähigkeit (logische Trennung von Daten unterschiedlicher Kunden)
- Funktionstrennung von Produktions-, Test- und Entwicklungsumgebungen
- klare Zuordnung von Zuständigkeiten und Verantwortlichkeiten

1.5 Pseudonymisierung (Art. 32 Abs. 1 Buchst. a DSGVO; Art. 25 Abs. 1 DSGVO)
Ein Personenbezug ist nur möglich, wenn zusätzliche Informationen hinzugezogen werden können.
- personenbezogene Daten werden, soweit möglich, unter einem Pseudonym gespeichert
- zusätzliche Informationen zur Identifizierung werden getrennt verarbeitet, sofern technisch umsetzbar

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

2.1. Weitergabekontrolle
Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle
- Verwendung verschlüsselter Netzwerkprotokolle (HTTPS/TLS)
- Absicherung der Datenübertragung durch aktuelle Transportverschlüsselung (z. B. TLS 1.2 oder höher)
- Protokollierung von Datenübermittlungen innerhalb der Systeme
- Vorgaben für sichere Passwortnutzung
- Übertragungen erfolgen ausschließlich über gesicherte Verbindungen

2.2. Eingabekontrolle
Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.
- systemseitige Protokollierungen

- Kontrolldaten werden aufbewahrt
- Zugriff auf die Protokolle ist nur Berechtigten möglich

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

Verfügbarkeitskontrolle
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
- Einsatz etablierter Cloud-Infrastrukturen zur Sicherstellung der Systemverfügbarkeit
- regelmäßige Aktualisierung von Systemen durch Sicherheits-Updates
- Einsatz von Schutzmechanismen (z. B. Firewalls, Zugriffsbeschränkungen)
- Monitoring der Systemverfügbarkeit und Performance
- automatisierte oder regelmäßig durchgeführte Sicherungsprozesse
- Überprüfung der Wiederherstellbarkeit der Daten im Rahmen technischer und organisatorischer Möglichkeiten
- redundante Speicherung innerhalb der genutzten Cloud-Infrastruktur
- Maßnahmen der eingesetzten Subdienstleister (z. B. Rechenzentrumsbetreiber) werden berücksichtigt

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

4.1 Datenschutz-Management
Der Auftragnehmer hat ein Verfahren im Einsatz, das die Beachtung des Datenschutzes sicherstellt.
- Handbuch/Richtlinien zum Datenschutz für Mitarbeitende vorhanden
- Datenschutzkoordinator ist benannt
- regelmäßige Kontrolle durch den Datenschutzkoordinator
- Beschäftigte werden im Datenschutz geschult und sind sensibilisiert
- Beschäftigten sind zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet
- interne Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst
- Verzeichnis von Verarbeitungstätigkeiten im Sinn des Art. 30 DSGVO wird geführt
- es finden verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen statt

4.2 Incident-Response-Management
Der Auftragnehmer hat ein Verfahren im Einsatz, das den Umgang mit datenschutzrechtlichen Vorfällen beschreibt.
- Vorgaben vorhanden, was als Datenpanne anzusehen ist
- Vorgaben vorhanden, wie mit Datenpannen umzugehen ist
- Dokumentation von Vorfällen
- Unterstützung des Verantwortlichen bei Meldepflichten
- Einsatz von Monitoring- und Logging-Mechanismen zur Erkennung von Systemanomalien und Sicherheitsvorfällen (ab Juli 2026)

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
Der Auftragnehmer hat ggf. ein Verfahren im Einsatz, mit dem datenschutzfreundliche Voreinstellungen gewährleistet werden.
- Rechte- und Rollenkonzept nach dem „Need to know“-Prinzip
- Vermeidung externer Ressourcen, soweit möglich und sinnvoll
- sparsame Datenerhebung
- keine automatische Verknüpfung von Daten und keine Profilbildung

4.4 Auftragskontrolle
Die weisungsgebundene Verarbeitung im Auftrag ist zu gewährleisten.
- eindeutige Vertragsgestaltung aufgrund von Musterverträgen
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung
- Subunternehmer werden in Textform beauftragt

Anlage 2.b:
Genehmigte Unterauftragsverhältnisse

zu Nr. 6.2 der Anlage 2 (Auftragsverarbeitung)

Weitere Auftragsverarbeiter	Anschrift / Land	Beschreibung der Datenverarbeitung
Amazon Web Services EMEA SARL	38, avenue John F. Kennedy, L-1855 Luxemburg	Hosting und Rechenzentrum; **die Datenverarbeitung findet in EU-Rechenzentren statt, zusätzlich ist der zugehörige US-Dienstleister nach TADPF zertifiziert**
Netlify, Inc.	512 2nd Street, Floor 2 San Francisco, CA 94107 United States	Bereitstellung von Hosting- und Deployment-Infrastruktur für die Webanwendung. **Die Datenverarbeitung erfolgt ausschließlich in der Region EU (Frankfurt).**
Neon, Inc.	160 Spear Street, 15th Floor, San Francisco, CA 94105 United States	Bereitstellung der Datenbank-Infrastruktur. **Die Datenverarbeitung erfolgt in der Region EU (Frankfurt).**
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Irland	ggf. nur im Einzelfall (z.B. Einsatz von Office-Lösung im Support); **die Datenverarbeitung findet in EU-Rechenzentren statt, zusätzlich sind EU-Standardvertragsklauseln abgeschlossen und der zugehörige US-Dienstleister ist TADPF-zertifiziert**