QuDaMed

Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Datenschutz nach Datenschutzgrundverordnung und Datenschutzanpassungs- und Umsetzungsgesetz

1. Rechtlicher Hintergrund
2. Grundsätze der Verarbeitung
3. Informationspflichten
4. Verzeichnisse von Verarbeitungstätigkeiten (VVT)
5. Vertraulichkeit und Integrität
6. Sonstiges
7. Fazit

Rechtlicher Hintergrund

Warum ist Datenschutz überhaupt ein Thema in der Arztpraxis?

Die gesetzlichen Regelungen finden sich z.B. an folgenden Stellen:

✓ EU Datenschutz Grundverordnung (DSGVO) und ab dem 28.05.2018 im Datenschutz-Anpassungs- und Umsetzungsgesetzt (DAnpUG-EU)

✓Strafgesetzbuch §203

Warum ist Datenschutz überhaupt ein Thema in der Arztpraxis?

Die gesetzlichen Regelungen finden sich z.B. an folgenden Stellen:

- ✓ SGB V §73 Absatz 1b
- ✓ Musterberufsordnung für Ärzte §10

DSGVO …

… EU-Verordnung zum Datenschutz, die bereits im Mai 2016 in Kraft getreten ist und bis zum 28.05.2018 umgesetzt werden muss.

DAnpUG-EU …

… wird die Neufassung des BDSG sein, welche ab dem 28.05.2018 Ergänzungen zur DSGVO enthalten wird.

Strafgesetzbuch §203 …

… regelt die Verletzung von Privatgeheimnissen.

Sozialgesetzbuch V §73 Absatz 1b …

… regelt die Einverständniserklärung des Patienten.

Musterberufsordnung für Ärzte §10 …

… regelt, welche Daten in welcher Form an den Patienten ausgehändigt werden müssen.

Grundsätzlich gilt, dass …

… alle im Gesundheitswesen erhobenen, verarbeiteten und genutzten Daten besondere Kategorien von Daten einzustufen sind.

… die Verarbeitung dieser Daten grundsätzlich erstmal untersagt ist.

… eine Ausnahme die Verarbeitung zum Zweck der Gesundheitsvorsorge ist, wenn das Fachpersonal dem Berufsgeheimnis unterliegt (§203 StGB).

Grundsätzlich gilt, dass …

… unter bestimmten Voraussetzungen ein Datenschutzbeauftragter benannt werden muss.

… bei der Verarbeitung personenbezogener Daten entsprechende Sicherheitsmaßnahmen zu treffen sind.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Grundsätze der Verarbeitung

gemäß DSGVO

- Auszug -

Artikel 5 „Grundsätze für die Verarbeitung personenbezogener Daten (pbD)“

- Datenminimierung ➔ werden pbD wirklich an allen Stellen benötigt, an welchen sie momentan verarbeitet werden?
  Es ist z.B. zu prüfen, ob die personenbezogenen Daten an den genutzten Geräten Softwareanwendungen durch Nummern ersetzt werden können.

Hierzu gehört aber auch, dass z.B. in Anamnesebögen gekennzeichnet werden muss, welche Angaben freiwillig sind und wofür diese benötigt werden (z.B. Telefonnummer und Mailadresse).

Werden an der Anmeldung Fotos für die Patientenakten gemacht, muss ebenfalls darauf hingewiesen werden, wofür diese benötigt werden und dass die Aufnahmen freiwillig sind.

Artikel 5 „Grundsätze für die Verarbeitung pbD“

- Speicherbegrenzung ➔ über die ggf. gesetzliche geforderte Frist hinaus dürfen pbD „…ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke…“ archiviert werden.

- Rechenschaftspflicht ➔ „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.“

Informationspflichten

Nach Artikel 13 und 14 der DSGVO sind allgemeine Informationen bzgl. der Datenverarbeitung vorzuhalten und zugänglich zu machen.

Gemäß DSAnpUG-EU müssen diese Informationen aber nicht persönlich übergeben werden, wenn die Informationen auf anderen Wegen öffentlich zur Verfügung gestellt werden.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Verzeichnisse von Verarbeitungstätigkeiten (VVT)

Die „alten“ Verarbeitungsübersichten werden abgelöst von den Verzeichnissen der Verarbeitungstätigkeiten (VVT).

Hier sind neben Angaben zur Zweckbindung auch Aussagen zu den jeweils getroffenen technisch-organisatorischen Maßnahmen (TOM) aufzuführen.

Die VVT können auch in Kategorien der Datenverarbeitung oder nach Schutzklassen zusammengefasst und erstellt werden.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Vertraulichkeit und Integrität

Da im medizinischen Bereich besondere Kategorien an Daten verarbeitet werden ist auch der Vertraulichkeit ein hoher Stellenwert einzuräumen.

Hierzu gehören z.B. folgende Punkte:

- Wird bei der Anschaffung von „smarten Geräten“ darauf geachtet, dass auch hier entsprechende Passwortrichtlinien beachtet werden und die Datenübertragung verschlüsselt erfolgt?

- Können die Patienten ihr Anliegen an der Anmeldung ohne neugierige Ohren vortragen können (Diskretionszonen und getrenntes Wartezimmer)?
- Werden Telefonate an einem separaten Telefonarbeitsplatz geführt? Wenn nein wird bei Telefonaten an der Anmeldung auf die Nennung von Namen verzichtet?

- Sind Bildschirme so aufgestellt, dass niemand „mitlesen“ kann?
- Werden Daten an Dritte (z.B. auch Versicherungen) nicht ohne schriftliche Einwilligung des Patienten weitergeleitet?
- Sind die Behandlungsräume entsprechend ausgestattet, dass Gespräche auf dem Flur oder im Wartezimmer nicht „mitgehört“ werden können?

- Ist sichergestellt, dass Patienten nicht unbefugt auf fremde Daten zugreifen können, wenn sie alleine im Behandlungszimmer sind (z.B. über passwortgeschützte Bildschirmschoner, keine Karteikarten unbeaufsichtigt liegen lassen,…)?
- Werden Arztberichte usw. nicht unverschlüsselt per Mail verschickt?
- Sind Aktenschränke abgeschlossen?

- Entsprechend die Passwortrichtlinien für die personenbezogenen Logins den aktuellen Erfordernissen, z.B. der 8-8-8-Regelung (8-stellig, alle 8 Monate zu wechseln, die letzten 8 Passwörter sind gesperrt)?
- Ist über ein Rollen- und Rechtekonzept sichergestellt, dass nicht alle auf alle Daten zugreifen können?

- Ist nachvollziehbar, wer wann welche Einträge vorgenommen oder verändert hat (Logfiles oder abzeichnen mit Datum und Kürzel)?
- Gibt es schriftliche Regelungen, dass keine privaten Geräte in das Praxisnetz gehängt werden dürfen?
- Ist sichergestellt, dass Antivirenprogramme stets automatisch aktualisiert werden?

Sonstiges

Vorhandene Dokumente müssen auf Verweise auf das „alte“ BDSG überprüft und entsprechend aktualisiert werden.

Hierzu gehören z.B.:

- Besucherlisten
- Einwilligungserklärungen
- Verpflichtungserklärungen / Arbeitsverträge

- Für die schriftlichen Vereinbarungen z.B. mit den Geräteherstellern oder Softwareanbietern (Vereinbarungen Auftragsverarbeitung) gibt es neue Vorgaben bzgl. der Inhalte
- Auch Geheimhaltungsvereinbarungen z.B. mit externen Reinigungsfirmen müssen ebenso aktualisiert werden wie die vorhandenen QM-Dokumente.

- Im Zuge der DSGVO müssen auch im Datenschutz Risikoanalysen durchgeführt werden, hier heißen diese Datenschutz-Folgeabschätzungen.
- Der Datenschutzbeauftragte muss bei der Behörde gemeldet werden. **Achtung:** Es gibt noch keine Meldeformulare!
- Datenschutzverstöße müssen bei der Behörde gemeldet werden. **Achtung:** Für den nicht-öffentlichen Bereich sind noch keine Meldeformulare veröffentlicht!

Fazit

- Wenn man sich aber erstmal einen Überblick verschafft hat, an welchen Stellen mit welchen Geräten und Anwendungen personenbezogene Daten verarbeitet werden, kann man die Erstellung der VVT´s und der ADV´s gut strukturieren.
- In Zusammenarbeit mit dem QM lassen sich Punkte wie die Datenschutz-Folgeabschätzungen und die notwendigen Datenschutzdokumente bearbeiten.

- Vorhandene Dokumente – auch z.B. Besucherlisten, Verpflichtungserklärungen für Mitarbeiter und Praktikanten müssen aktualisiert und an die DSGVO angepasst werden.

Es gibt viel zu tun – an einer Stelle muss man einfach anfangen!

Vielen Dank

für Ihre Aufmerksamkeit

und

Ihr Interesse

QuDaMed

Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Sonnemann / Strelecki GbR

Anke Sonnemann / Joachim Strelecki

Kronenstr. 77

44139 Dortmund

Tel.: 0231 / 97 86 9 - 51 / 52

Fax: 0231 / 97 86 9 - 53

E-Mail: info@qudamed.de

Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO[1]

Hinweis:
Diese Formulierungshilfe ist nicht abschließend und bezieht sich in erster Linie auf die Fallgestaltung einer Auslagerung von klassischen IT-Dienstleistungen z. B. für die Lohnabrechnung oder Finanzbuchhaltung.
Je nach konkretem Anwendungsfall müssen gegebenenfalls weitere Inhalte hinzukommen, können solche weggelassen oder müssen modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden (z. B. bei Berufsgeheimnisträgern, bei Dienstleistungen zur Wartung, Datenlöschung oder -konvertierung, bei der externen Datenarchivierung).

Auftraggeber (Verantwortlicher):

.....

Auftragnehmer (Auftragsverarbeiter):

.....

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

.....

(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

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

Dauer des Auftrags

Der Vertrag beginnt am ..... und endet am .....

[1] Diese Formulierungshilfe stellt keine Standardvertragsklauseln im Sinne von Art. 28 Abs. 8 DS-GVO dar.

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist .....

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

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

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen

technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

.....

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

.....

(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

.....

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

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

5. Pflichten des Auftragnehmers

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

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

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

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

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

.....

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:
……..

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

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

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

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Ein-

holung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

.....

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

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

.....

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

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

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

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

.....

(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Sofern einschlägig:
Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

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

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

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

(Hinweis: Hier sind verschiedene Regelungsalternativen möglich. Die Parteien können ein absolutes Unterauftragsverbot vereinbaren, es kann aber auch ein Verbot mit Genehmigungsvorbehalt im Einzelfall geregelt werden. Auf letztere Möglichkeit bezieht sich der unten stehende Formulierungsvorschlag.)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

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

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

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

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

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

.....

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage ..... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

(Hier haben die Vertragsparteien einen Gestaltungsspielraum: Entweder werden dem Auftragnehmer allgemein Befugnisse eingeräumt, Subunternehmer zu beauftragen oder dies wird von einer Einzelgenehmigung abhängig gemacht. Einigt man sich auf eine allgemeine Befugnis des Auftragnehmers zur Beauftragung von Subunternehmern, ist jede Subbeauftragung vorher durch den Auftragnehmer dem Auftraggeber anzuzeigen. Der Auftraggeber hat dann von Gesetzeswegen ein Recht auf Einspruch gegen diese Änderung (Art. 28 Abs. 2). Das Recht des Auftraggebers zum Einspruch ist im Vertrag ausdrücklich zu erwähnen. Da das Gesetz die Folgen dieses Einspruchs nicht regelt, wird empfohlen, hierzu vertragliche Regelungen zu finden. Wird keine Regelung getroffen, ist die Bestellung des Unterauftragnehmers, gegen den Einspruch erhoben wurde, nicht möglich.)

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck

der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:
……

Das im Anhang …….. beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das im Anhang ……. beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:

> Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden am …… durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:
> ……
> Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

Oder:

> Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

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

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

dem Auftraggeber auszuhändigen.

oder

wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

.....

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

.....

11. Haftung

Auf Art. 82 DS-GVO wird verwiesen.
Im Übrigen wird folgendes vereinbart:

.....

12. Vertragsstrafe

Bei Verstoß des Auftragnehmers gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro vereinbart.

13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Weitere Beispiele für mögliche Regelungen:

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Datum:

Unterschriften

Auftraggeber	Auftragnehmer

Praxis Dr. Mustermann Musterstaße Musterhausen Tel.:	**Informationen bzgl. der Erhebung und Verarbeitung personenbezogener Daten**			
	Nr. FB-D 001	Version 01	Gültig ab 31.05.2017	Seite 1 von 1

Sehr geehrte Patienten,

Ihre personenbezogenen Daten (Name, Vorname, Geburtsdatum, Anschrift, Versichertendaten) benötigen wir, um die von Ihnen gewünschten Untersuchungen durchführen zu können, Arztbriefe erstellen zu können und die erbrachten Leistungen abrechnen zu können.

In diesem Zusammenhang werden Ihre Daten ggf. an weitere Stellen weitergeleitet. Dies können z.B. die KV zur Abrechnung oder das Fremdlabor für relevante Blutuntersuchungen sein, welche wir nicht selbst durchführen können. Sollte eine dieser Datenübermittlungen nicht auf einer gesetzlichen Grundlage beruhen, stellen wir Ihnen natürlich im Vorfeld eine entsprechende Einwilligungserklärung zur Verfügung, damit Sie Ihr Einverständnis schriftlich bestätigen können. Diese Einverständniserklärung enthält selbstverständlich einen Hinweis auf das Ihnen zustehende Widerrufsrecht.

Sie haben jederzeit das Recht, Einsicht in Ihre Daten zu wünschen. Bitte sprechen Sie uns kurz an, damit wir einen entsprechenden Termin vereinbaren können. Sollte Ihnen im Rahmen dieser Akteneinsicht auffallen, dass uns bei der Erhebung Ihrer Daten ein Fehler unterlaufen ist, so korrigieren wir dies natürlich umgehend. Bitte beachten Sie, dass wir Daten nicht auf Wunsch löschen können, da wir gemäß den gesetzlichen Vorgaben z.B. aus der Musterberufsordnung für Ärzte verpflichtet sind, Ihre Daten 10 Jahre zu archivieren, bevor diese vernichtet werden können. Vor Ablauf dieser vorgeschriebenen Aufbewahrungspflicht können Sie lediglich eine Einschränkung der Datenverarbeitung beantragen, welche jedoch auch erst ab dem Datum des Antrags gilt.

Bei weiteren Fragen können Sie sich auch gerne jederzeit an unseren Datenschutzbeauftragten Herrn Datenschutz wenden. Die Kontaktdaten stellen wir Ihnen auf Anfrage zur Verfügung.

Besucherliste

Datum	Name, Vorname	Firma	Zu Besuch bei	Unterschrift *

* Durch Ihre Unterschrift bestätigen Sie, dass Sie auf allgemeine Datenschutzregelungen hingewiesen wurden und diese einhalten.

Labor Musterhausen	DSFA nach SDM			
	Nr. FB037	Version 01	Gültig ab	Seite 1 von 4

Beschreibung des zu prüfenden Bereichs (z.B. Anschaffung eines neuen Gerätes, Einführung einer neuen Analyse / Umstellung einer Methode, Einführung neuer Arbeitsabläufe,…)

Nr.	Frage	Beschreibung	Schweregrad (A)	Auftretenswahr-scheinlichkeit (B)	Risikoindex (A x B)	Kennung Beurteilung	Maßnahmen
Sachliche Verhältnisse							
1	Wer trägt die Verantwortung?						
2	Erfolgt die Verarbeitung zur Erfüllung der Aufgabe einer öffentlichen Stelle?						
3	Besteht ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis einer verantwortlichen privaten Stelle mit den Betroffenen?						
4	Bilden Einwilligungen der Betroffenen die Rechtsgrundlage der Verarbeitung und, wenn ja, welchen Inhalt haben sie und wie werden sie eingeholt?						
5	Wenn mehrere Stellen oder Auftragsdatenverarbeiter in die Verarbeitung involviert sind, wie sind dann die Rechtsverhältnisse zwischen ihnen geregelt?						
6	Für welche Zwecke erfolgt die Verarbeitung und welche Geschäftsprozesse der verantwortlichen Stelle(n) werden durch sie unterstützt?						

Beurteilung der möglichen Risiken

Schweregrad	1 = zu vernachlässigen	2 = signifikant	3 = schwerwiegend	4 = kritisch	5 = katastrophal
Auftretenswahrscheinlichkeit	1 = fast nie	2 = selten	3 = gelegentlich	4 = häufig	5 = nahezu immer

Beurteilung Risikoindex:	1-7: allgemein vertretbares Risiko = A	8 - 14: vertretbares Risiko, Maßnahmen erforderlich = B	15 - 25: unvertretbares Risiko = C	entfällt = e

Nr.	Frage	Beschreibung	Schweregrad (A)	Auftretenswahr-scheinlichkeit (B)	Risikoindex (A x B)	Kennung Beurteilung	Maßnahmen
7	Welche Daten werden in welchen Schritten und unter Nutzung welcher Systeme und Netze und der Kontrolle welcher Personen erhoben, verarbeitet und genutzt?						
8	Welche Hilfsprozesse werden zur Unterstützung der Verarbeitung betrieben?						
9	Welche technische Infrastruktur wird genutzt?						
	Materiellrechtliche Bewertung						
10	Welches Recht ist auf die Verarbeitung anzuwenden?						
11	Welche Zwecke können mit der Verarbeitung legitim verfolgt werden und welche Zweckänderungen sind im Zuge der Verarbeitung zulässig?						
12	Welche Daten sind für die Erfüllung der zulässigen Zwecke erheblich bzw. erforderlich?						
13	Welche Befugnisse bestehen zur Übermittlung von Daten zwischen den beteiligten Stellen und von diesen an Dritte?						
14	Welchen Beschränkungen unterliegt die Offenbarung von verarbeiteten Daten an Personen innerhalb und außerhalb						

Beurteilung der möglichen Risiken

Schweregrad	1 = zu vernachlässigen	2 = signifikant	3 = schwerwiegend	4 = kritisch	5 = katastrophal
Auftretenswahrscheinlichkeit	1 = fast nie	2 = selten	3 = gelegentlich	4 = häufig	5 = nahezu immer

Beurteilung Risikoindex:	1-7: allgemein vertretbares Risiko = A	8 - 14: vertretbares Risiko, Maßnahmen erforderlich = B	15 - 25: unvertretbares Risiko = C	entfällt = e

Nr.	Frage	Beschreibung	Schweregrad (A)	Auftretenswahr-scheinlichkeit (B)	Risikoindex (A x B)	Kennung Beurteilung	Maßnahmen
	der beteiligten Stellen?						
15	Welchen besonderen Anforderungen müssen die technischen und organisatorischen Maßnahmen genügen?						
	Gewährleistungsziele						
16	Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten?						
17	Welche Daten sollen unversehrt, welche aktuell gehalten werden?						
18	Wem ist die Kenntnisnahme welcher Daten zu verwehren?						
19	Für wen ist die Datenverarbeitung in welcher Form transparent zu halten?						
20	Welche Betroffenenrechte sind in welcher Ausprägung zu gewähren?						
21	Welche Zweckänderungen sind zulässig? Welche Zwecke von Hilfsprozessen leiten sich aus den Kernprozessen legitim ab?						
22	Die Kenntnisnahme von und die Ausübung welcher Verfügungsgewalt über welche Daten der Betroffenen durch welche Personen und Stellen sind zu minimieren?						
	Schutzbedarfsanalyse						

Beurteilung der möglichen Risiken

Schweregrad	1 = zu vernachlässigen	2 = signifikant	3 = schwerwiegend	4 = kritisch	5 = katastrophal
Auftretenswahrscheinlichkeit	1 = fast nie	2 = selten	3 = gelegentlich	4 = häufig	5 = nahezu immer

Beurteilung Risikoindex:	1-7: allgemein vertretbares Risiko = A	8 - 14: vertretbares Risiko, Maßnahmen erforderlich = B	15 - 25: unvertretbares Risiko = C	entfällt = e

Nr.	Frage	Beschreibung	Schweregrad (A)	Auftretenswahr-scheinlichkeit (B)	Risikoindex (A x B)	Kennung Beurteilung	Maßnahmen
normal	□						
hoch	□						
sehr hoch	□						

Beurteilung Risikoindex:	1-7: allgemein vertretbares Risiko	8 - 14: vertretbares Risiko, Maßnahmen erforderlich	15 - 25: unvertretbares Risiko

Zusammenfassung der Risikoabschätzung / Beurteilung / Festlegungen von Anforderungen an die Methodenvalidierung

Gesamtbeurteilung:	
Datum, Unterschrift ärztliche Leitung:	

Beurteilung der möglichen Risiken

Schweregrad	1 = zu vernachlässigen	2 = signifikant	3 = schwerwiegend	4 = kritisch	5 = katastrophal
Auftretenswahrscheinlichkeit	1 = fast nie	2 = selten	3 = gelegentlich	4 = häufig	5 = nahezu immer

Beurteilung Risikoindex:	1-7: allgemein vertretbares Risiko = A	8 - 14: vertretbares Risiko, Maßnahmen erforderlich = B	15 - 25: unvertretbares Risiko = C	entfällt = e

Übersichtsliste Dienstleister & Lieferanten

1 Firma	2 Art der Dienstleistung	3 Werden pbD übermittelt?	4 Wenn ja zu welchem Zweck	5 Können vor Ort pbD eingesehen werden?	6 Wenn ja zu welchem Zweck?	7 Geheimhaltung (GH) oder ADV
						□ GH □ ADV

Achtung, Spalte 7 ist durch die Datenschutzbeauftragten auszufüllen

Übersicht Verarbeitung pbD an den Geräten

1 Bezeichnung des Gerätes	2 Werden pbD an das Gerät geschickt?	3 Rohdaten elektronisch oder Papier?	4 Zeitraum Archivierung Rohdaten	5 gesetzliche Grundlage für Rohdatenarchiv?	6 Wenn ja welche?	7 Geheimhaltung (GH) oder ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV

Achtung, Spalte 7 ist durch den Datenschutzbeauftragten oder Datenschutzbevollmächtigten auszufüllen

Übersicht Verarbeitung pbD mittels Softwareprodukten

1 Bezeichnung der Software	2 Werden pbD geschickt / verarbeitet?	3 Rohdaten?	4 Zeitraum Archivierung Rohdaten	5 gesetzliche Grundlage für Rohdatenarchiv?	6 Wenn ja welche?	7 Geheimhaltung (GH) oder ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV
	☐ ja ☐ nein	☐ elek. ☐ Papier		☐ ja ☐ nein		☐ GH ☐ ADV

Achtung, Spalte 7 ist durch den Datenschutzbeauftragten oder Datenschutzbevollmächtigten auszufüllen

Einverständniserklärung

Hiermit erkläre ich, _____

Name, Vorname Geburtsdatum

mich damit einverstanden, dass meine Daten zu folgenden Zwecken an folgende Stellen weitergeleitet werden:

- → Auftragslaboratorien* zum Zweck der Untersuchung labormedizinischer Parameter, die wir bei uns nicht durchführen können
- → Pathologie*
- → Privatärztliche Verrechnungsstelle*
- → … bitte ergänzen

Ich bin damit einverstanden, dass Rezepte von folgenden Personen in meinem Namen abgeholt werden dürfen:

_____

_____

Ich bin damit einverstanden, dass Sie zusätzlich zu mit- und weiterbehandelnden Ärzten folgenden Personen telefonisch Auskunft bzgl. meiner Daten geben dürfen:

_____

_____

Ich bin berechtigt, gemäß SGB V §73 Absatz 1b diese Einverständniserklärung jederzeit zu widerrufen.

_____

Datum / Unterschrift

* Die genauen Anschriften sind beim Personal der Anmeldung zu erfragen.

Einverständniserklärung

Hiermit erkläre ich, _____

Name, Vorname Geburtsdatum

mich damit einverstanden, dass meine Daten zu folgenden Zwecken an folgende Stellen weitergeleitet werden:

- → Auftragslaboratorien* zum Zweck der Untersuchung labormedizinischer Parameter, die wir bei uns nicht durchführen können
- → Pathologie*
- → Privatärztliche Verrechnungsstelle*
- → … bitte ergänzen

Ich bin damit einverstanden, dass Rezepte von folgenden Personen in meinem Namen abgeholt werden dürfen:

_____

_____

Ich bin damit einverstanden, dass Sie zusätzlich zu mit- und weiterbehandelnden Ärzten folgenden Personen telefonisch Auskunft bzgl. meiner Daten geben dürfen:

_____

_____

Ich bin berechtigt, gemäß SGB V §73 Absatz 1b diese Einverständniserklärung jederzeit zu widerrufen.

_____

Datum / Unterschrift

* Die genauen Anschriften sind beim Personal der Anmeldung zu erfragen.

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)

Frau / Herr _____
wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogenen Daten müssen

a. auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d. sachlich richtig und erforderlichenfalls auf dem neusten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur solange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden erforderlich ist;
f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und / oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsrechtlichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadensersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- und Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtungen wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.
Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

_____ _____

Ort, Datum Unterschrift Mitarbeiter/in

Verzeichnis von Verarbeitungstätigkeiten

Bezeichnung des Verfahrens	Verarbeitung der pbD an Analysengeräten
Name und Kontaktdaten des Verantwortlichen	Labor Dr. Mustermann Dr. Mustermann Musterstraße Musterhausen Tel.: E-Mail:
Name und Kontaktdaten des Datenschutzbeauftragten	Herr / Frau Beispiel Beispielstraße Beispielhausen Tel.: E-Mail
Zwecke der Verarbeitung	Die pbD werden im Rahmen der Durchführung der angeforderten Analytik zusammen mit den Untersuchungskürzeln an den Geräten verarbeitet.
Beschreibung der Kategorien betroffener Personen	Patienten
Beschreibung der Kategorien personenbezogener Daten	Name, Vorname, ggf. Geburtsdatum
Kategorien von Empfängern	Ggf. Gesundheitsämter oder RKI im Rahmen von Meldepflichten
Ggf. Übermittlungen an ein Drittland	Bei international agierenden Firmen werden in entsprechenden Verträgen Regelungen enthalten, dass pbD nicht in Drittländer übermittelt werden dürfen.
Fristen für die Löschung	Gemäß den im Rahmen des QM festgelegten Fristen werden Rohdaten zur Sicherstellung der Überprüfung der Richtigkeit und Integrität der Daten für XXX aufbewahrt, bevor die Daten gelöscht werden.
TOM gemäß DSGVO Artikel 32 Absatz 1	
Pseudonymisierung und Verschlüsselung pbD	Eine Pseudonymisierung der Daten erfolgt aus Gründen der Sicherheit nicht.
Wahrung der Vertraulichkeit	Techniker, die im Rahmen von Reparaturen oder Wartungen theoretisch Einsicht in die Daten nehmen könnten werden in der Besucherliste auf die Vertraulichkeit hingewiesen und unterschreiben dies. Weiterhin sind entsprechende Regelungen auch bzgl. der Wahrung der Vertraulichkeit der Daten im Rahmen von Fernwartungen in oben aufgeführten Verträgen enthalten.
Wahrung der Integrität	Werden Geräte neu mittels online an das LIS angeschlossen erfolgt eine Vorabkontrolle der Onlines nach vordefinierten Kriterien. Eine arbeitstägliche Überprüfung der Funktionalität und der Wahrung der Integrität erfolgt im

	Rahmen der Auswertung der täglichen internen Qualitätskontrolle. Die Dokumentation der jeweils genutzten Gerätesoftware erfolgt in den Formblättern zur Gerätedokumentation und Geräteüberwachung.
Wahrung der Verfügbarkeit der Daten	An den Analysengeräten werden nach Bedarf Datensicherungen durchgeführt bzw. Rohdaten ausgedruckt. Die genauen Informationen werden in den Geräteanweisungen hinterlegt.
Wahrung der Belastbarkeit der Systeme und Dienste	Im Rahmen der Auswahl der Geräte wird neben Zeiten der Analysendauer auch die anfallende Datenmenge und Kommunikationsgeschwingdigkeiten und -wege überprüft.