Vertrag zur Auftragsverarbeitung zwischen

NAKO e.V.
Am Taubenfeld 21/2
69123 Heidelberg
– nachfolgend Auftraggeberin genannt –

und

Firma/Studienzentrum/Kompetenzeinheit
Anschrift
PLZ Ort
– nachfolgend Auftragnehmerin genannt –

Name und Kontaktdaten des Datenschutzbeauftragten der Auftraggeberin	Dr. iur. Christian Borchers datenschutz süd GmbH Wörthstraße 15 97082 Würzburg 0931 304 976 0 office@datenschutz-sued.de
Name und Kontaktdaten des Datenschutzbeauftragten der Auftragnehmerin (sofern benannt)	Bitte angeben

§ 1 Gegenstand und Dauer des Auftrags

(1) Die Auftragnehmerin führt die in Anlage 1 beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

§ 2 Weisungen der Auftraggeberin

(1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.

(5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und in Anlage 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.

(3) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(6) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihre bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin

besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn die Auftraggeberin dies vorher schriftlich genehmigt hat.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

(4) Die Inanspruchnahme der in Anlage 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte der Auftraggeberin

Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße der Auftragnehmerin

Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin. Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Die Auftraggeberin kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die Auftragnehmerin einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeberin aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände der Auftraggeberin ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

_____	_____
Ort, Datum	Auftraggeberin
_____	_____
Ort, Datum	Auftragnehmerin

Anlage 1 Studienzentrum / Institution etc.

Umfang, Art und Zweck der vorgesehenen Verwendung der Daten

(1) Der Auftragnehmer führt im Rahmen des Vertragsgegenstands, für die Dauer des Auftrags und ausschließlich im Rahmen der getroffenen Vereinbarungen folgende Aufgaben in Bezug auf die im Studienzentrum rekrutierten bzw. untersuchten Probanden durch:

a) im Rahmen des Probandenmanagements:

- Verwaltung der personenidentifizierenden Daten der potentiellen Probanden, der Probanden und Nichtteilnehmer (Datenaustausch mit den örtlich zuständigen Meldebehörden und der unabhängigen Treuhandstelle der NAKO, Abklärung offener Fragen wie z.B. bei Verdacht auf doppelte Ziehung einer Person in den Melderegisterstichproben)
- Rekrutierung (Abfrage Adresslisten, Ziehung nach Vorgabe des Studienprotokolls, Einladung und Terminverwaltung)
- Führung der lokalen Response-Statistik
- Ansprechpartner für Kontakt zu den Probanden (u. a. Beantwortung von Nachfragen von Probanden, Versand von Ergebnismitteilungen)
- Archivierung anfallender Papierdokumente (z. B. ausgedruckte und unterschriebene Einwilligungserklärungen)

b) im Rahmen der Untersuchungseinheit:

- standardisierte Datenerhebung: Dokumentation der Aufklärung und Einwilligung, Abgleich, Ergänzung und Korrektur von Kontaktdaten zur Übermittlung an das Probandenmanagement, Eingabe von Untersuchungsergebnissen der Probanden in elektronische Formulare (eCRFs), Scannen von Fragebögen, Gerätedaten-Import, Ablaufdokumentation
- standardisierte Gewinnung von Probenmaterial: Gewinnung, Verarbeitung, Lagerung und Versand von Bioproben inkl. Dokumentation.

c) ggf. ergänzen:

- _____

(2) Der Auftragnehmer verarbeitet im Rahmen seines Auftrags die folgenden personenbezogenen Daten in Bezug auf die im Studienzentrum rekrutierten bzw. untersuchten Probanden:

- *Personenidentifizierende Daten* (Name, Geburtsdatum, Geschlecht, Kontaktdaten wie beispielsweise Wohnanschrift, Telefonnummern und E-Mail-Adressen): Diese Daten dienen der Identifikation einer Person und zur Kontaktierung dieser Person. Sie werden in der Probandenmanagement- und Terminverwaltungssoftware im Probandenmanagement langfristig gespeichert und an die unabhängige Treuhandstelle übermittelt. Im Zusammenhang mit der Untersuchung kann die Untersuchungseinheit temporär Zugriff auf diese Daten erhalten, sie abgleichen ergänzen und korrigieren.
- *Einwilligung:* Die freiwillige, informierte Einwilligung der betroffenen Person ist Voraussetzung für die Teilnahme als Proband an der NAKO. Die Einwilligung wird in der Regel durch die Untersuchungseinheit eingeholt und dokumentiert. Widerrufe werden in der Regel durch das Probandenmanagement verarbeitet.
- *Geburtsdatum und Geschlecht* werden darüber hinaus für die Überprüfung der korrekten Zuordnung pseudonymisierter Daten und zur Steuerung des Untersuchungsablaufs verwendet. Dafür werden diese Angaben zusätzlich in der Studiendatenbank in den Integrationszentren gespeichert. Angaben zum Alter (in ganzen Jahren und in Altersgruppen) werden auch im Rahmen der wissenschaftlichen Auswertung verwendet.
- *Kontaktinformationen:* Die Studienzentren führen eine vollständige Historie der Kontakt-versuche und Kontakte zu den in den Stichproben der Meldebehörden enthaltenen Personen. Dies dient der Optimierung einer Re-Kontaktierung der betreffenden Personen, der Logistik des Informations- und Materialaustauschs mit Probanden (z. B. Verwaltung vom Probanden zurück zu sendender Geräte, Versand des Ergebnisbriefs), in anonymisierter Form der Auswertung der Response einschließlich ggf. zur Verbesserung der Response erforderlicher Anpassungen des Rekrutierungsprozesses.

- *Weitere identifizierende Daten:* Name und Adresse der Krankenversicherung, Krankenversicherungsnummer und die Sozial-/Rentenversicherungsnummer werden als Identifikatoren für die Gewinnung von Sekundärdaten von externen Datenquellen in der Untersuchungseinheit erhoben und an die unabhängige Treuhandstelle übermittelt.
- *Weitere Adressdaten, Geolokalisierung:* Wohn- und Arbeitsadressen für die Zuordnung von Daten hinsichtlich der Umweltexpositionen der Studienteilnehmer.
- *Befragungs- und Gesundheitsdaten einschließlich Daten bildgebender Verfahren* werden in der Untersuchungseinheit nach einem detaillierten, standardisierten Protokoll pseudonymisiert erhoben und verarbeitet. Als Erhebungsinstrumente kommen selbstbeantwortete oder untersucherunterstützte Fragebögen, Interviews, Untersuchungen mit oder ohne Einsatz diagnostischer Geräte zum Einsatz. Die Erfassung erfolgt weitgehend automatisiert (Web-Formulare, Touchscreen, Import von Daten diagnostischer Geräte etc.) Die Erhebung und Verarbeitung dieser Daten wird automatisiert dokumentiert. Diese Daten inkl. Dokumentation werden unmittelbar, wo dies technisch nicht möglich ist, zeitnah an die Studiendatenbank in den Integrationszentren übermittelt und nicht langfristig im Studienzentrum gespeichert. Für Zwecke der Qualitätssicherung erhält das Studienzentrum Zugriff auf die in der Studiendatenbank gespeicherten Daten.
- *Bioproben:* Die Bioproben werden in der Untersuchungseinheit nach einem detaillierten, standardisierten Protokoll gewonnen, aufbereitet, zwischengelagert und in das zentrale Biorepository der NAKO oder das dezentrale Bioprobenlager versandt. Eine Blutprobe wird zur sofortigen Analyse an das unten genannte lokale Labor übergeben.
- *Weitere Befragungs- und Gesundheitsdaten sowie Bioproben* können nach Maßgabe der Ordnung des NAKO e.V. zur Durchführung von Level 3-Projekten der NAKO im Rahmen eigener Forschungsprojekte des Studienzentrums gewonnen werden und müssen gesondert vertraglich geregelt sein.
- *Befragungs- und Gesundheitsdaten sowie Bioproben* können durch das Studienzentrum nach Maßgabe der Nutzungsordnung des NAKO e.V. zur Nutzung von Daten und Probenmaterial der NAKO für eigene Forschungsprojekte verwendet werden.

(3) Weitere Vorschriften
Die folgenden Dokumente mit Weisungscharakter sind in der jeweils gültigen Fassung Bestandteil dieses Vertrages:

- SOPs;
- Nutzungsordnung des NAKO e.V. zur Nutzung von Daten und Probenmaterial der NAKO;
- Ordnung des NAKO e.V. zur Durchführung von Level 3-Projekten der NAKO;
- Datenschutz- und IT-Sicherheitskonzept der NAKO;
- Konzept der Unabhängigen Treuhandstelle der NAKO;
- Nutzungsbedingungen für Daten zur Qualitätssicherung in der NAKO.

(4) Die Datenverarbeitung findet an folgenden Orten statt: (Hier konkrete Adresse/n)

- Probandenmanagement: …
- Untersuchungseinheit: …
- Lokales Labor: …
- Dezentrales Bioprobenlager: …

(5) Weisungsberechtigte Personen des Auftraggebers sind:

Der Vorstand des NAKO e.V.

Weisungsempfänger beim Auftragnehmer sind:

Bitte entspr. Namen angeben

Anlage 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.

Anlage 3: Technisch-organisatorische Maßnahmen

A. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	Zutrittskontrollmaßnahmen zu Serverräumen
1.0	Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betriebenen werden? ☐ ja ☐ nein
	Wenn 1.0 nein: In diesem Fall müssen die weiteren Fragen zu A1 nicht beantwortet werden, sondern sogleich die Fragen ab A2. Auch die Fragen zu B1 und B2 entfallen.
1.1	Standort des Serverraums / Rechenzentrums (RZ). Klicken Sie hier, um Text einzugeben.
1.2	Sind die personenbezogenen Daten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)? ☐ ja ☐ nein
1.3	**Falls 1.2 ja: Machen Sie bitte die entsprechenden Standortangaben auch bzgl. weiterer Server.** Weitere Serverstandorte: Klicken Sie hier, um Text einzugeben.
1.4	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für **alle** im Einsatz befindlichen Server- / RZ Standorte? ☐ ja ☐ nein
1.5	**Falls 1.4 nein: Beantworten Sie bitte die Fragen 1.6 bis 1.21 und B für weitere RZ- / Serverstandorte.**
1.6	Ist der Serverraum fensterlos? ☐ ja ☐ nein
1.7	Wenn 1.6 nein: Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: bitte eintragen
1.8	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☐ nein
1.9	Wenn 1.8 ja: Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.10	Ist der Serverraum videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☐ nein
1.11	**Wenn 1.10 ja, mit Bildaufzeichnung**: Wie lange werden die Bilddaten gespeichert? bitte Wert in Tagen eintragen Tage
1.12	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: bitte Anzahl der Personen angeben Funktion im Unternehmen: bitte fortlaufend Funktion im Unternehmen angeben
1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☐ ja ☐ nein, mit mechanischem Schloss
1.14	**Wenn 1.13 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☐ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: bitte eintragen
1.15	**Wenn 1.13 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☐ ja ☐ nein

1.16	**Wenn 1.13 ja**: Werden die Zutritte zum Raum im Zutrittssystem protokolliert? ☐ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	**Wenn 1.16 ja**: Wie lange werden die Zutrittsdaten ungefähr gespeichert? bitte Wert in Tagen eintragen Tage
1.18	**Wenn 1.13 nein**, wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus? Anzahl Schlüssel: Schlüsselanzahl Aufbewahrungsort: Aufbewahrungsort eintragen Ausgabestelle: bitte Ausgabestelle angeben
1.19	Aus welchem Material besteht die Zugangstür zum Serverraum? ☐ Stahl / Metall ☐ sonstiges Material
1.20	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja ☐ nein
1.21	**Wenn 1.20 ja**: Was wird in dem Serverraum noch aufbewahrt? ☐ Telefonanlage ☐ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv ☐ Lagerung von IT Ausstattung ☐ Sonstiges: bitte eintragen
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.
2.	**Zutrittskontrollmaßnahmen zu Büroräumen**
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: bitte Standorte eintragen
2.2	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? ☐ ja ☐ nein
2.3	Wird ein Besucherbuch geführt? ☐ ja ☐ nein
2.4	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☐ nein
2.5	**Wenn 2.4 ja**: Wer wird informiert, wenn die EMA auslöst? ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
2.6	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☐ nein
2.7	**Wenn 2.6 „ja, mit Bildaufzeichnung“,** wie lange werden die Bilddaten gespeichert? bitte Wert in Tagen eintragen Tage
2.8	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? ☐ ja, Gebäude und Büroräume sind elektronisch verschlossen

	☐ ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage. ☐ ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☐ nein
2.9	**Wenn 2.8 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☐ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: bitte eintragen
2.10	**Wenn 2.8 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☐ ja ☐ nein
2.11	**Wenn 2.8 ja**: Werden die Zutritte im Zutrittssystem protokolliert? ☐ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche positive Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht
2.12	**Wenn 2.11 ja**: Wie lange werden diese Protokolldaten aufbewahrt? bitte Wert in Tagen eintragen Tage
2.13	**Wenn 2.11 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich
2.14	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☐ ja ☐ nein
2.15	**Wenn 2.14 ja**: Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus? ☐ ja ☐ nein Ausgabestelle: bitte Ausgabestelle angeben
2.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☐ nein ☐ ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.
3.	**Zugangs- und Zugriffskontrollmaßnahmen**
3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? ☐ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: bitte angeben
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? ☐ ja ☐ nein
3.2	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☐ ja ☐ nein

3.3	Existieren verbindliche Passwortparameter im Unternehmen? ☐ ja ☐ nein
3.4	**Passwort-Zeichenlänge:** bitte angeben **Muss das Passwort Sonderzeichen enthalten?** ☐ ja ☐ nein **Mindest-Gültigkeitsdauer in Tagen:** bitte angeben
3.5	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? ☐ ja ☐ nein
3.6	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Wenn ja, nach wieviel Minuten? bitte Wert in Minuteneintragen Minuten
3.7	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? ☐ Admin vergibt neues Initialpasswort ☐ keine
3.8	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☐ ja, bitte Anzahl eintragen Versuche ☐ nein
3.9	**Wenn 3.8 ja**, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für bitte Wert in Minuteneintragen Minuten gesperrt.
3.10	Wie erfolgt die Authentisierung bei Fernzugängen: Authentisierung mit ☐ Token ☐ VPN-Zertifikat ☐ Passwort
3.11	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☐ ja, bitte Anzahl eintragen Versuche ☐ nein
3.12	**Wenn 3.11 ja**, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für bitte Wert in Minuteneintragen Minuten gesperrt.
3.13	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? ☐ ja, nach bitte Wert in Minuteneintragen Minuten ☐ nein
3.15	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert? ☐ ja ☐ nein
3.16	**Wenn 3.15 ja:** Wird die Firewall regelmäßig upgedatet? ☐ ja ☐ nein
3.17	**Wenn 3.15 ja**: Wer administriert Ihre Firewall? ☐ eigene IT ☐ Externer Dienstleister
3.18	**Wenn ein externer DL zum Einsatz kommt**: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? ☐ ja ☐ nein, die Aufschaltung ist nur im 4 Augenprinzip mit einem Mitarbeiter der eigenen IT möglich.
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der

	Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.
4.	**Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten**
4.1	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) entsorgt? ☐ Altpapier / Restmüll ☐ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. ☐ Sonstiges: bitte angeben
4.2	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt? ☐ Physikalische Zerstörung durch eigene IT. ☐ Physikalische Zerstörung durch externen Dienstleister. ☐ Löschen der Daten ☐ Löschen der Daten durch bitte Anzahl angeben Überschreibungen ☐ Sonstiges: bitte angeben
4.3	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) ☐ ja ☐ nein
4.4	Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden? ☐ generell ja ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. ☐ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.
4.6	Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt? ☐ Verschlüsselung der Festplatte ☐ Verschlüsselung einzelner Verzeichnisse ☐ keine Maßnahmen
4.7	Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)? ☐ ja ☐ nein
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.

5.	**Maßnahmen zur sicheren Datenübertragung**
5.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ gar nicht ☐ nein, Datenübertragung erfolgt per mpls ☐ nur vereinzelt ☐ per verschlüsselter Datei als Mailanhang ☐ per PGP/SMime ☐ per verschlüsseltem Datenträger ☐ per VPN ☐ per https/TLS ☐ per SFTP ☐ Sonstiges: bitte angeben
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☐ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister
5.2	Werden die Übertragungsvorgänge protokolliert? ☐ ja ☐ nein
5.3	**Wenn 5.2 ja**: Wie lange werden diese Protokolldaten aufbewahrt? bitte Wert in Tagen eintragen Tage
5.4	**Wenn 5.2 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.

B. Maßnahmen zur Sicherstellung der Verfügbarkeit

1.	**Serveraum**
1.1	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür? ☐ ja ☐ nein
1.2	Ist der Serverraum mit Rauchmeldern ausgestattet? ☐ ja ☐ nein
1.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? ☐ ja ☐ nein
1.4	Ist der Serverraum mit Löschsystemen ausgestattet? **Mehrfachantworten möglich!** ☐ ja, CO2 Löscher ☐ ja, Halon / Argon Löschanlage ☐ Sonstiges: bitte angeben
1.5	Woraus bestehen die Außenwände des Serverraumes? ☐ Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise ☐ Brandschutzwand (bspw. F90)
1.6	Ist der Serverraum klimatisiert? ☐ ja ☐ nein
1.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? ☐ ja ☐ nein
1.8	Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert? ☐ ja ☐ nein
1.9	Werden die Funktionalität 1.2, 1.3, 1.4, 1.6, 1.7 und 1.8, sofern vorhanden, regelmäßig getestet? ☐ ja ☐ nein
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.
2.	**Backup- und Notfall-Konzept, Virenschutz**
2.1	Existiert ein Backupkonzept? ☐ ja ☐ nein
2.2	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet? ☐ ja ☐ nein
2.3	In welchem Rhythmus werden Backups vom Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? ☐ Echtzeitspiegelung ☐ täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: bitte angeben
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert? ☐ Zweiter redundanter Server ☐ Sicherungsbänder ☐ Festplatten ☐ Sonstiges: bitte angeben
2.5	Wo werden die Backups aufbewahrt? ☐ Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, datenträger- und

	dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch ☐ Im Serverraum ☐ Privathaushalt ☐ Sonstiges: bitte Art der Aufbewahrung angeben
2.6	**Zu 2.5:** Im Falle eines Transports der Backups: Wie wird dieser durchgeführt? ☐ Mitnahme durch einen MA der IT / Geschäftsleitung / Sekretärin ☐ Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen) ☐ Sonstiges: bitte angeben
2.7	Sind die Backups verschlüsselt? ☐ ja ☐ nein
2.8	Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil? ☐ ja ☐ nein
2.9	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? ☐ ja ☐ nein ☐ Prozess existiert, ist jedoch nicht dokumentiert
2.10	**Wenn 2.9 ja**, wer ist für das Software- bzw. Patchmanagement verantwortlich? ☐ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister
2.11	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? ☐ ja ☐ nein
2.12	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem ☐ Virenschutz ☐ Anti-Spyware ☐ Spamfilter
2.13	**Wenn 2.13 ja**, wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich? ☐ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.
3.	**Netzanbindung**
3.1	Verfügt das Unternehmen über eine redundante Internetanbindung? ☐ ja ☐ nein
3.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☐ ja ☐ nein
3.3	Wer ist für die Netzanbindung des Unternehmens verantwortlich? ☐ eigene IT ☐ Externer Dienstleister
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos

	für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: Klicken oder tippen Sie hier, um Text einzugeben.

_____ _____

Ort & Datum **Unterschrift des Auftragnehmers**

Hinweis:

Bei Änderungen der von Ihnen getroffenen und hier dokumentierten technischen – organisatorischen Sicherheitsmaßnahmen sind die Änderungen dem Auftraggeber unverzüglich mitzuteilen. Diese Anlage ist dann entsprechend zu aktualisieren, mit dem aktuellen Tagesdatum zu versehen und durch Abstimmung mit dem Auftraggeber unter Ersetzung der Vorversion zum neuen Vertragsbestandteil zu machen.