Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG

zwischen

Nationale Kohorte e.V.

– nachfolgend gemäß § 11 Abs.1 BDSG **Auftraggeber** genannt –

und

[Kompetenzeinheitsbetreiber]

– nachfolgend gemäß § 11 Abs. 2 BDSG **Auftragnehmer** genannt –

Präambel

Die Nationale Kohorte (NaKo) ist ein gemeinsames interdisziplinäres Vorhaben von Wissenschaftlern aus der Helmholtz-Gemeinschaft, den Universitäten und anderen Forschungsinstituten in Deutschland. Ihr Ziel ist die Untersuchung der Entwicklung der wichtigsten chronischen Krankheiten (Krankheiten des Herz-Kreislaufsystems und der Lunge, Diabetes, Krebs, neurodegenerative/-psychiatrische und Infektionskrankheiten), ihrer subklinischen Vorstufen und funktionellen Veränderungen.

Für die NaKo werden 200.000 Studienteilnehmer - Männern und Frauen im Alter von 20 bis 69 Jahren - aus verschiedenen Regionen Deutschlands rekrutiert. Für eine Subgruppe innerhalb der Kohorte von 40.000 Männern und Frauen ist ein intensiviertes Untersuchungsprotokoll vorgesehen. Rekrutierung und Nachbeobachtung der Teilnehmer der NaKo werden von 18 lokalen Studienzentren in acht geographischen Clustern, verteilt über fast alle deutschen Bundesländer, durchgeführt. Die Studienzentren bestehen jeweils aus den Einheiten Probandenmanagement und Untersuchungseinheit

Der Nationale Kohorte e.V. hat als satzungsgemäße Aufgabe die Durchführung dieser repräsentativ angelegten bevölkerungsbezogenen Langzeitbeobachtung und deren Nutzbarmachung für die Erforschung der Ursachen von Volkskrankheiten im Zusammenspiel von genetischer Veranlagung, Lebensgewohnheiten und umweltbedingten Faktoren. Die Durchführung der Studie stützt sich dabei auf das den internationalen Gutachtern vorgelegte Wissenschaftliche Konzept (http://www.nationale-kohorte.de/wissenschaftliches-konzept.html), sowie den Förderantrag für die ersten 5 Jahre des Projekts (**BMBF Förderkennzeichen 01ER1301A).**

Der Nationale Kohorte e.V. hat als Auftraggeber i.S.d. § 11 Abs. 1 BDSG am 27.09.2012 ein Datenschutzkonzept mit dem Bundesdatenschutzbeauftragten abgestimmt, welches am 13.03.2013 nochmals bestätigt wurde. Dieses Datenschutzkonzept bildet die Grundlage für nachfolgende Vereinbarung. Danach ist verantwortliche Stelle, d.h. Daten verarbeitende Stelle der Auftraggeber. Die Verantwortung für die Durchführung der Basisuntersuchung und der Wiederholungsuntersuchungen in den Studienzentren liegt ausschließlich beim Auftraggeber. Die 18 Studienzentren, die beiden Integrationszentren, die Kompetenzeinheiten und die Transferstelle führen die Datenverarbeitung im Auftrag des Auftraggebers durch. Zur Regelung der Einzelheiten der Datenverarbeitung im Auftrag schließen der Auftraggeber und der Auftragnehmer folgenden Vertrag:

§ 1 Vertragsgegenstand und Dauer der Vereinbarung

(1) Gegenstand dieses Vertrages ist das Erheben, Verarbeiten und Nutzen (gemeinsam „**Verwenden**“) der im Probandenmanagement und der Untersuchungseinheit des Auftragnehmers im Rahmen der in der Vereinssatzung (§2 (1)) genannten Langzeitbeobachtung („**Nationale Kohorte“) anfallenden und im Wissenschaftlichen Konzept (**http://www.nationale-kohorte.de/wissenschaftliches-konzept.html), sowie in der Deutschen Vorhabenbeschreibung des Projekts (**BMBF Förderkennzeichen 01ER1301A).** näher spezifizierten personenbezogenen Daten im Auftrag des Auftraggebers. Der Auftraggeber hat den Auftragnehmer unter Beachtung der Sorgfaltspflichten des § 11 Bundesdatenschutzgesetz (BDSG) als Dienstleister ausgewählt. Dieser

Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsdatenverarbeitung i.S.d. § 11 BDSG und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verwendung der Daten.
Hinsichtlich einer konkreten Beschreibung des Vertragsgegenstandes für den o.g. Auftragnehmer wird auf die Dokumentation in der entsprechenden Standard Operating Procedure (SOP) in der jeweils gültigen Fassung verwiesen.
(2) Der Einfachheit halber stellen die Vertragspartner klar, dass nach ihrem Verständnis die Formulierung „personenbezogene Daten“ in den nachfolgenden Regelungen nicht nur personenbezogene Daten i. S. d. BDSG erfasst, sondern auch Sozialdaten i. S. d. SGB X.
(3) Art, Umfang und Zweck der vorgesehenen Datenverwendung ist im Anhang 1 zu diesem Vertrag verbindlich festgelegt. Änderungen, die sich im Laufe der Zeit im Projekt ergeben könnten, sind in einer schriftlichen Vereinbarung zwischen den Parteien vorab festzulegen.
(4) Dieser Vertrag tritt mit Unterzeichnung beider Parteien in Kraft und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von einem Monat zum Quartalsende kündbar. Er endet jedoch nicht vor Erfüllung der Lösch- und Rückgabepflichten nach § 12. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

§ 2 Zulässigkeit der Datenverarbeitung

Der Auftraggeber ist alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchgeführten Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer.

§ 3 Weisungsgebundenheit

Der Auftragnehmer ist bei der Auftragserfüllung zur Verarbeitung personenbezogener Daten in allen Phasen nur im Rahmen der Weisungen des Auftraggebers berechtigt. Diese Weisungen bedürfen der Schriftform. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten ausschließlich für den Zweck, für den sie entsprechend der Weisungen des Auftraggebers zu verwenden sind.

Weisungsberechtigte und Weisungsempfänger sind im Anhang zu diesem Vertrag aufgeführt. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich oder in Textform der Nachfolger bzw. der Vertreter mitzuteilen.

Zur Durchführung des Vertragsgegenstandes ist der Auftragnehmer zur Durchführung aller technisch erforderlichen Verarbeitungen (z. B. Duplizieren von Beständen zur Verlustsicherung, Auslesen von Log-files, etc.) berechtigt, soweit die Verarbeitung nicht zu einer inhaltlichen Umgestaltung führt.

§ 4 Gegenseitige Hinweispflicht

Der Auftragnehmer hat den Auftraggeber unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung gegen das BDSG oder andere Vorschriften über den Datenschutz verstößt. Er ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis die Weisung – nach erfolgtem Hinweis – durch den Auftraggeber bestätigt oder geändert wurde.

Auftragnehmer und Auftraggeber werden sich gegenseitig unverzüglich informieren, wenn Störungen, Unregelmäßigkeiten oder der Verdacht auf Datenschutzverletzungen auftreten.

Der Auftragnehmer richtet solche Hinweise über die Geschäftsstelle des Auftraggebers an den Vorstand und den Datenschutzbeauftragten des Auftraggebers.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn

der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

§ 5 Verpflichtung auf das Datengeheimnis

Der Auftragnehmer ist verpflichtet, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 5 BDSG zu wahren.

Er hat hierzu bei der Verarbeitung und Nutzung ausschließlich Beschäftigte einzusetzen, die auf das Datengeheimnis verpflichtet sind. Er hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken (Schulung/Unterweisung), dass alle Personen, die mit der Erfüllung des Vertrages betraut sind oder sonst Zugriff zu den personenbezogenen Daten haben könnten, die gesetzlichen Bestimmungen über den Datenschutz kennen, verstanden haben und beachten.

§ 6 Datenschutzbeauftragter

Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Beauftragten für den Datenschutz Beim **Auftragnehmer** ist **Frau/Herr [Name] als [betrieblicher|behördlicher|institutioneller] Beauftragter für den Datenschutz** bestellt. Sie/Er nimmt eine beratende Funktion bei der Ausführung des BDSG sowie anderer Vorschriften zum Datenschutz im Hinblick auf das Auftragsverhältnis beim Auftragnehmer ein. Stellt die/der Datenschutzbeauftragte bzw. die Institution selbst in diesem Zusammenhang Unregelmäßigkeiten fest, ist unverzüglich der Auftraggeber zu informieren.

§ 7 Rechte der Betroffenen

Die Rechte der durch die Datenverarbeitung beim Auftragnehmer betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte. Der Auftragnehmer hat den Auftraggeber bei der Wahrung dieser Rechte, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung im Rahmen seiner Möglichkeiten zu unterstützen.

§ 8 Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem Bundesdatenschutzgesetz oder anderer Vorschriften über den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung oder -nutzung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich.
Der Auftragnehmer stellt den Auftraggeber frei von Ansprüchen nach Maßgabe der § 7 BDSG, § 82 SGB X, die ihm als Daten verarbeitende Stelle in Durchführung dieses Vertrages entstehen, soweit der Auftragnehmer diese zu vertreten hat.

§ 9 Pflichten

Der Auftragnehmer ist verpflichtet, eine aktuelle, detaillierte Dokumentation der Datenverarbeitung oder -nutzung vorzuhalten, anhand derer der Auftraggeber den Nachweis über die ordnungsgemäße Durchführung der Datenverarbeitung oder Nutzung führen kann.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner bei der Verarbeitung personenbezogener Daten bestehenden Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und entsprechende Nachweise zu führen.

Die Verantwortung für den Transport der Daten obliegt dem Auftraggeber.

Der Auftragnehmer weist dem Auftraggeber die von ihm üblicherweise eingerichteten Verlustsicherungsmaßnahmen nach. Zusätzliche Anforderungen des Auftraggebers und daraus resultierende Maßnahmen sind schriftlich zu vereinbaren. Der Auftragnehmer sichert dem Auftraggeber die ordnungsgemäße Vernichtung nicht benötigten Datenmaterials zu (Probeausdrucke,

überzählige Listen, etc.). Der Auftragnehmer sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen des Auftragnehmers getrennt aufbewahrt, verarbeitet und genutzt werden.

§ 10 Auftragskontrolle

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durchführen zu lassen.

Als Verantwortlicher für die Durchführung der Auftragskontrolle wird auf Seiten des Auftraggebers der Datenschutzbeauftragte Dr. Christian Borchers und dessen Erfüllungsgehilfen (datenschutz süd GmbH) benannt. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel 24 Stunden vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

§ 11 Unterauftragsverhältnisse

Sollen weitere Unterauftragsverhältnisse zur Auftragserfüllung abgeschlossen werden, ist hierüber der Auftraggeber vor einer entsprechenden Vereinbarung zu unterrichten. Das Unterauftragsverhältnis kann nur dann abgeschlossen werden, wenn der Auftraggeber diesem schriftlich unter genauer Bezeichnung des Unterauftragnehmers und des Auftragsgegenstandes zugestimmt hat und die Datenschutzbestimmungen dem Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Die Zustimmung wird dann Bestandteil dieses Vertrages.

§ 12 Verpflichtung über das Vertragsende hinaus

Bei Beendigung des Auftragsverhältnisses hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Datenträger und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen und personenbezogene Daten enthalten – hierunter fallen auch Gesundheitsdaten und Bioproben – an den Auftraggeber zurückzugeben bzw. in Absprache mit dem Auftraggeber zu vernichten und einen Nachweis der ordnungsmäßigen Vernichtung zu führen. Die genannten Daten und alle weiteren personenbezogenen Daten vom Auftraggeber sind unverzüglich zu löschen, es sei denn der Löschung stehen gesetzliche Speicherfristen entgegen.

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

Der Auftragnehmer hat im Regressfall dem Auftraggeber auch nach Vertragsende die noch vorhandenen Dokumentationen zur Führung des Entlastungsbeweises nach § 7 BDSG zu überlassen. Die Vertragsparteien sind verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus Stillschweigen über die im Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren.

§ 13 Festlegung der technischen und organisatorischen Maßnahmen

Der Auftragnehmer ist verpflichtet, bei der Verarbeitung der Daten des Auftraggebers die Vorschriften des BDSG, insbesondere des § 9 „Technische und organisatorische Maßnahmen“ und der Anlage zu § 9 BDSG zu beachten und umzusetzen.
Die folgenden technischen und organisatorischen Maßnahmen werden gem. § 9 BDSG und dessen Anlage verbindlich durch den Auftraggeber im Anhang zu diesem Vertrag festgelegt:

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

Der Auftragnehmer verpflichtet sich, für alle Verfahren, die sich auf personenbezogene Daten beziehen, Verfahrensbeschreibungen gem. der Anlage zu § 9 Satz 1 BDSG zu erstellen, welche die lokalen Besonderheiten beschreiben (vgl. Anlage 2). Diese Verfahrensbeschreibungen sind dem Auftraggeber über dessen Geschäftsstelle unaufgefordert zur Verfügung zu stellen.

Die technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses entsprechend der technischen und organisatorischen Weiterentwicklung im Bereich des Auftragnehmers fortzuschreiben.

Werden grundlegende Änderungen der technischen und organisatorischen Maßnahmen vorgenommen, sind diese zunächst mit dem Datenschutzbeauftragten des Auftraggebers abzustimmen. Der Auftraggeber muss vor Durchführung der Änderung dieser zustimmen. Die Änderungen sind schriftlich zu fixieren und werden Vertragsbestandteil.

§ 14 Wirksamkeit der Vereinbarung

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

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlage 1 Studienzentrum

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.

(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 Nationalen Kohorte. 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 Nationalen Kohorte 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 Nationale Kohorte e.V. zur Durchführung von Level 3-Projekten der Nationalen Kohorte 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 Nationale Kohorte e.V. zur Nutzung von Daten und Probenmaterial der Nationalen Kohorte für eigene Forschungsprojekte verwendet werden.

(3) Weitere Vorschriften
Die folgenden Dokumente mit Weisungscharakter sind Bestandteil dieses Vertrages:

- SOPs in der jeweils gültigen Fassung
- Nutzungsordnung des Nationale Kohorte e.V. zur Nutzung von Daten und Probenmaterial der Nationalen Kohorte vom 27.02.2013
- Ordnung des Nationale Kohorte e.V. zur Durchführung von Level 3-Projekten der Nationalen Kohorte

(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 Nationale Kohorte e.V.:

Prof. Dr. Karl-Heinz Jöckel

Prof. Dr. Wolfgang Ahrens

Prof. Dr. Wolfgang Hoffmann

Prof. Dr. Rudolf Kaaks

Henrik Becker

Weisungsempfänger beim Auftragnehmer sind:

.....

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers

§ 9 Bundesdatenschutzgesetz:

„Technische und organisatorische Maßnahmen
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

***Anlage** (zu § 9 Satz 1)*
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

*1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),*

*2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),*

*3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),*

*4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),*

*5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),*

*6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),*

*7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),*

*8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. (Einhaltung des **Trennungsprinzips**)“*

Hinweis:

Bei Änderungen der von Ihnen getroffenen und hier im Folgenden zu dokumentierenden technischen – organisatorischen Sicherheitsmaßnahmen sind diese Änderungen dem Auftraggeber unverzüglich mitzuteilen. Dieser Anhang 2 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.

Bitte machen Sie nur zu den Fragen Angaben machen, die für Ihre Dienstleistung relevant sind.

1. Zutrittskontrolle

Serverseitig umgesetzte Zutrittskontrollmaßnahmen:

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
1.1	Sind die Auftragsdaten auf mehr als einen Serverstandort verteilt sind (bspw. Backup Server)?	☐ ja ☐ nein	Falls ja: Machen Sie unter 1.1.1 die entsprechenden Adressangaben auch bzgl. weiterer Server.	keine
1.1.1	Nennen Sie bitte die genaue Adresse / -n des / der Standorte /-s der / -s Serverraums.		keine	keine
1.1.2	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Server?	☐ ja ☐ nein	Falls 1.1.2 Nein: Nehmen Sie Kontakt zum AG aus. Dieser wird Ihnen entsprechende Muster zur Verfügung stellen, um die Maßnahmen differenziert darzustellen.	keine
1.2	Wird der Server durch den Auftragnehmer (AN) selbst, oder durch einen Dienstleister / Subunternehmer des AN betrieben?	☐ Auftragnehmer ☐ Dienstleister	Sofern der Server durch einen Subunternehmer betrieben wird, nennen Sie bitte Namen und Sitz des Dienstleisters!	
1.3	Im wievielten Stock liegt der Serverraum?	☐ EG ☐ Keller __ OG (bitte Geschoss-zahl eintragen)	keine	keine
1.4	Ist der Serverraum fensterlos?	☐ ja ☐ nein	Wenn nein, wie sind die Fenster vor Einbruch geschützt?	☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht
1.5	Ist der Serverraum alarmgesichert?	☐ ja ☐ nein	Wenn ja, von wann bis wann ist die Anlage aktiviert?	Bitte Wert eintragen!

				_____ Uhr abends bis _____ Uhr morgens
1.6	Ist der Serverraum mit einem elektronischen Schließsystem versehen?	☐ ja ☐ nein	Wenn ja, handelt es sich um ein PIN gestütztes, oder ein RFID gestütztes System?	☐ RFID ☐ PIN Wenn PIN: Anzahl Zeichen: _____ Gültigkeitsdauer der PIN: _____ Monate
1.7	Wenn 1.6 ja: Sind die Zutrittskarten / PIN Nummern personenbezogen vergeben / personifiziert?	☐ ja ☐ nein	keine	keine
1.8	Wenn 1.6 ja: werden die Zutritte zum Raum im Zutrittssystem gespeichert.	☐ ja ☐ nein	Wenn ja, für wie lange?	Bitte Wert eintragen! _____ Tage _____ Wochen _____ Monate _____ Jahre
1.9	Wenn 1.6 ja: Werden negative Zutrittsversuche ebenfalls gespeichert?	☐ ja ☐ nein		
1.10	Wenn 1.8 und / oder 1.7 ja: Wie viele Personen haben Zugriff auf die Zutritts Protokolldaten	Bitte Wert eintragen! _____ Personen	Nennen Sie die Funktionen der Personen mit Zugriffs auf die Zutritts-protokolldaten:	Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____
1.11	Existiert ein mechanisches Schloss.	☐ ja ☐ nein	Wenn ja, wie viele Schlüssel existieren und wo werden diese aufbewahrt.	Bitte Wert eintragen! Anzahl Schlüssel: _____
1.12	Wenn 1.11 ja: Wird die Schlüsselausgabe protokolliert?	☐ ja ☐ nein	Wenn 1.11 und 1.12 ja: Wie wird protokolliert und wer gibt die Schlüssel aus?	☐ Schlüsselbuch Ausgabestelle: _____
1.13	Wie viele Personen haben Zutritt zum Serverraum?	Bitte Wert eintragen!	Nennen Sie die Funktionen der	☐ gleiche Funktionen wie bei 1.10

		_____ Personen	Zutrittsberechtigten:	☐ oder: Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____
1.14	Ist der Serverraum videoüberwacht?	☐ ja ☐ nein	Wenn ja, wo und wie lange werden die Bilddaten gespeichert?	Bitte Wert eintragen! _____ Tage Speicherort: _____
1.15	Wenn 1.14 ja: Wer hat Zugriff auf die Videodaten der Serverraum-überwachung?	☐ gleiche Funktionen wie bei 1.10 ☐ oder: Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____	Wenn 1.14 ja: Wird der Zugriff auf die Bilddaten der Videoüberwachung protokolliert?	☐ ja ☐ nein
1.16	Wie ist der Zutritt durch betriebsfremde Personen zum Serverraum geregelt? (bspw. im Falle von Wartungsdiensten / Elektrikern).	☐ es gibt keine Regelung hierzu ☐ Zutritt und Anwesenheit nur in Begleitung	Werden Zutritte durch Betriebsfremde protokolliert?	☐ ja ☐ nein
1.17	Aus welchem Material besteht die Zugangstür zum Serverraum?	☐ Stahl ☐ sonstiges Metall ☐ Holz ☐ sonstiges Material	keine	keine
1.18	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt?	☐ ja ☐ nein	Wenn 1.18 ja: Was wird in dem Serverraum noch aufbewahrt?	☐ Telefonanlage ☐ Lagerung Büromaterial ☐ Lagerung von Akten ☐ Archiv ☐ Lagerung von IT Ausstattung ☐ Sonstiges: _____

Clientseitig umgesetzte Zutrittskontrollmaßnahmen:

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
1.19	Nennen Sie bitte die genaue Adresse des Standortes der Clients, von denen aus auf die Daten des Auftraggebers zugegriffen werden kann.	Adresse:	keine	keine
1.20	Im wievielten Stock liegen die Büroräume?	☐ EG ☐ Keller _____OG	keine	keine
1.21	Existiert ein Pförtner- / Empfangsdienst?	☐ ja ☐ nein	Handelt es sich um eigene MA oder einen externen Dienstleister:	☐ Eigene MA ☐ externer DL
1.22	Wird ein Besucherbuch geführt?	☐ ja ☐ nein	Wenn ja, welche Daten werden hier aufgenommen und wie lange werden die Eintragungen aufbewahrt?	☐ Name ☐ Uhrzeit des Aufenthalts (von – bis) ☐ Ansprechpartner im Haus ☐ Besuchsgrund ☐ Firma ☐ Unterschrift des Besuchers ☐ Zeichen / Unterschrift des Pförtners Aufbewahrungszeit: _____
1.23	Ist das Bürogebäude alarmgesichert?	☐ ja ☐ nein	Wenn ja, von wann bis wann ist die Anlage aktiviert?	Bitte Wert eintragen! ☐ Uhr abends bis ☐ Uhr morgens
1.24	Ist das Bürogebäude mit einem elektronischen Schließsystem versehen?	☐ ja ☐ nein	Wenn ja, handelt es sich um ein PIN gestütztes, oder ein RFID gestütztes System?	☐ RFID ☐ PIN Wenn PIN: Anzahl Zeichen: ☐ Gültigkeitsdauer der PIN:

				_____
1.25	Wenn 1.24. ja: Sind die Zutrittskarten / PIN Nummern personenbezogen vergeben)	☐ ja ☐ nein	keine	keine
1.26	Wenn1.24. ja: Werden die Zutritte zu den definierten Zutrittsbereichen gespeichert?	☐ ja ☐ nein	Wenn ja, für wie lange?	Bitte Wert eintragen! ☐ Tage ☐ Wochen ☐ Monate ☐ Jahre
1.27	Wenn 1.24. ja: Werden negative Zutrittsversuche ebenfalls gespeichert?	☐ ja ☐ nein		
1.28	Sind die Eingangsbereiche zum Gebäude videoüberwacht?	☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☐ nein	Wenn ja, mit Bildaufzeichnung: Wo und wie lange werden die Bilddaten gespeichert?	Bitte Wert eintragen! _____ Tage Ort: _____
1.29	Wenn 1.28 ja: Wer hat Zugriff auf die Videodaten der Videoüberwachung des Gebäudes?	☐ gleiche Personen wie bei 1.10 ☐ oder: Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____	Wenn 1.28 ja: Wird der Zugriff auf die Bilddaten der Videoüberwachung protokolliert?	☐ ja ☐ nein

2. Zugangskontrolle

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
2.1	Existiert ein kombinierter Passwort (PW)-Benutzername-Zugangsschutz der Systeme?	☐ ja ☐ nein	keine	keine
2.2	Wie werden die Zugangsberechtigungen vergeben?	☐ auf Antrag (schriftlich oder Mail) an IT ☐ Antrag muss durch Vorgesetzten	keine	keine

		genehmigt sein		
2.3	Geben Sie verbindliche Passwortparameter im Unternehmen vor?	☐ ja ☐ nein	keine	keine
2.4	Wie lauten die Passwort (PW) Vorgaben:	**Länge** des PW: ☐ weniger als 6 Zeichen ☐ weniger als 8 Zeichen ☐ 8 Zeichen oder länger Anzahl notwendiger Großbuchstaben: ☐ gar nicht ☐ 1 ☐ mehr als 1 Anzahl notwendiger Kleinbuchstaben: ☐ gar nicht ☐ 1 ☐ mehr als 1 Anzahl notwendiger Zahlen: ☐ gar nicht ☐ 1 ☐ mehr als 1 Anzahl notwendiger Sonderzeichen: ☐ gar nicht ☐ 1 ☐ mehr als 1 Gültigkeitsdauer des PW: ☐ 30 bis 60 Tage ☐ 60 - 90 Tage ☐ mehr als 90 Tage	keine	keine
2.5	Nach wie vielen Zyklen darf ein Nutzer dasselbe PW erneut vergeben	☐ keine Vorgabe ☐ 3 Zyklen	keine	keine

	(Passworthistorie)?	☐ 5 Zyklen ☐ mehr als 5 Zyklen		
2.6	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben?	☐ ja ☐ nein	Wenn nein, wie kontrollieren Sie die Einhaltung der PW Vorgaben?	☐ gar nicht ☐ Stichproben
2.7	Ist eine automatische PW geschützte Bildschirmsperre eingestellt.	☐ ja ☐ nein	Existieren Vorgaben zum Sperren des Clients beim Verlassen des Arbeitsplatzes?	☐ ja, der Rechner ist manuell zu sperren ☐ nein
2.8	Kontrollieren Sie die Aktualität der Zugangsberechtigungen?	☐ ja ☐ nein	Keine	keine
2.9	Welche Maßnahmen ergreifen Sie bei Verlust / Vergessen / Ausspähen eines PW?	☐ Admin setzt neues PW, dass der Nutzer dann nach Erstanmeldung zu ändern hat. ☐ keine	Keine	keine
2.10	Gibt es eine Begrenzung von Anmeldeversuchen mit einem Benutzernamen / PW?	☐ ja, weniger als 3 Versuche ☐ ja, weniger als 6 Versuche ☐ nein	Wenn ja, für wie lange?	Bitte Wert eintragen: Sperrung für _____ Minuten
2.11	Bei Fernzugängen (VPN / IPSec): Wie lauten hier die PW-Parameter?	**Länge** des PW: ☐ weniger als 6 Zeichen ☐ weniger als 8 Zeichen ☐ 8 Zeichen oder länger Anzahl notwendiger Großbuchstaben: ☐ gar nicht ☐ 1 ☐ mehr als 1 Anzahl notwendiger Kleinbuchstaben: ☐ gar nicht ☐ 1	Keine	keine

		☐ mehr als 1 Anzahl notwendiger Zahlen: ☐ gar nicht ☐ 1 ☐ mehr als 1 Anzahl notwendiger Sonderzeichen: ☐ gar nicht ☐ 1 ☐ mehr als 1 Gültigkeitsdauer des PW: ☐ 30 bis 60 Tage ☐ 60 - 90 Tage ☐ mehr als 90 Tage		
2.12	Wie viele MA haben über Fernzugänge Zugang auf die Daten des AG?	Bitte Wert eintragen: _____ Personen	Keine	keine
2.13	Nach wie vielen Fehlversuchen wird der Fernzugang gesperrt?	☐ ja, weniger als 3 Versuche ☐ ja, weniger als 6 Versuche ☐ nein	Wenn ja, für wie lange?	Bitte Wert eintragen: Sperrung für _____ Minuten
2.14	Wird der Fernzugang nach Inaktivität automatisch getrennt?	☐ ja ☐ nein	Wenn ja, wie lange muss die Inaktivität dauern, bis der Zugang getrennt wird?	Bitte Wert eintragen: Dauer der Inaktivität _____ Minuten
2.15	Gibt es eine getrennte Internet Struktur für Besucher?	☐ ja ☐ nein	keine	

3. Zugriffskontrolle

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
3.1	Existiert ein differenzierendes Berechtigungskonzept?	☐ ja ☐ nein	Wenn ja, ist dies mit Rollenbeschreibungen dokumentiert?	☐ ja ☐ nein
3.2	Wie werden die	☐ auf Antrag	keine	keine

	Zugriffsberechtigungen vergeben?	(schriftlich oder Mail) an IT ☐ Antrag muss durch Vorgesetzten genehmigt sein		
3.3	Gibt es für einzelne Speicherorte / Verzeichnisse weitere Zugriffsschutzmaßnahmen?	☐ ja, Verzeichnisse mit Kundendaten sind zusätzlich verschlüsselt. ☐ nein	keine	keine
3.4	Existieren getrennte Produktiv- und Testsysteme im Falle der Notwendigkeit der Wartung der Systeme?	☐ ja ☐ nein	keine	keine
3.5	Verfügt Ihr IT System über eine Firewall.	☐ ja ☐ nein	Wenn 3.5 ja: Wird die Firewall regelmäßig upgedatet?	☐ ja ☐ nein
3.6	Wenn 3.6 ja: Wer administriert Ihre Firewall?	☐ eigene IT ☐ Externer Dienstleister	Wenn ein externer DL zu Einsatz kommt: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten?	☐ ja ☐ nein
3.7	Wie werden nicht mehr benötigte Datenträger in Ihrem Unternehmen entsorgt?	☐ Physikalische Zerstörung durch eigene IT. ☐ Physikalische Zerstörung durch externen Dienstleister. ☐ Elektromüll	Wenn ein externer DL hierfür zum Einsatz kommt: Haben Sie einen Vertrag gem. § 11 BDSG (Auftragsdatenverarbeitung / ADV) mit diesem abgeschlossen?	☐ ja ☐ nein
3.8	Werden Zugriffe auf Daten des AG personenbezogen protokolliert?	☐ ja ☐ nein	Wenn 3.8 ja: Wer hat Zugriff auf diese Zugriffsprotokolle?	☐ gleiche Funktionen wie bei 1.10 ☐ oder: Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____

3.9	Werden Vergabe / Änderungen von Zugriffsberechtigungen protokolliert?	☐ ja ☐ nein	Wenn 3.9 ja: Wer hat Zugriff auf diese Zugriffsprotokolle?	☐ gleiche Funktionen wie bei 1.10 ☐ oder: Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____

4. Weitergabekontrolle:

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
4.1	Wie werden die Daten **vom AG an den AN** übertragen?	☐ VPN ☐ IPSec ☐ https / SSL ☐ http ☐ mobiler Datenträger ☐ E-Mail ☐ Fax ☐ Schriftlich ☐ telefonisch ☐ remote access ☐ Einsichtnahme am Monitor	Wenn die Daten elektronisch weitergegeben werden, erfolgt der Transfer verschlüsselt?	☐ nein ☐ nein, aber persönliche Übergabe ☐ nein, aber per PW geschütztem ZIP Archiv / Mailanhang ☐ ja, per PGP ☐ ja, per verschlüsselten Datenträger
4.2	Wie werden die Daten **vom AN an den AG** übertragen?	☐ VPN ☐ IPSec ☐ https / SSL ☐ mobiler Datenträger ☐ E-Mail ☐ Fax ☐ Schriftlich ☐ telefonisch ☐ remote access	Wenn die Daten elektronisch weitergegeben werden, erfolgt der Transfer verschlüsselt?	☐ nein ☐ nein, aber persönliche Übergabe ☐ nein, aber per PW geschütztem ZIP Archiv / Mailanhang ☐ ja, per PGP ☐ ja, per verschlüsselten Datenträger
4.3	Gibt es eine Vereinbarung, welche Personen auf Seite des AG und des AN die Daten übertragen dürfen?	☐ ja ☐ nein	Wenn 4.3 ja: Wer ist jeweils zur Übertragung von Auftragsdaten befugt?	**Für den AN:** _____ _____ Name & Funktion

				Für den AG: _____ _____ Name & Funktion
4.5	Werden die Übertragungsvorgänge protokolliert?	☐ ja ☐ nein	keine	keine
4.6	Werden Auftragsdaten auch auf mobilen Endgeräten verarbeitet?	☐ ja ☐ nein	Wenn 4.6 ja: Wie sind die Endgeräte, bzw. die darauf gespeicherten Auftragsdaten gesichert.	☐ gar nicht. ☐ gar nicht, da die Daten zwar mit den Geräten verarbeitet werden, aber nicht auf diesen gespeichert sind. ☐ Verschlüsselung der Festplatten / Verzeichnisse gem. modernen Standards. ☐ Zusätzlicher PW Schutz der Verschlüsselten Festplatten / Verzeichnisse.

5. Eingabekontrolle

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
5.1	Werden die Eingaben / Veränderungen / Löschungen von Auftragsdaten personenbezogen protokolliert?	☐ ja, elektronisch ☐ ja, papierbasiert ☐ nein	Wenn 5.1 ja: Wer hat Zugriff auf diese Protokolldaten?	☐ gleiche Funktionen wie bei 1.10 ☐ oder: Funktion:_____ Funktion:_____ Funktion:_____ Funktion:_____
5.2	Wenn 5.1 nein: Ist zumindest der letzte Zugriff auf die Daten (Uhrzeit / Datum der Änderung) feststellbar?	☐ ja ☐ nein	keine	keine

6. Auftragskontrolle

Nr.	Frage:	Antwort	Folgefrage	Antwort
6.1	Hat Ihr Unternehmen einen gem. §4g Bundesdatenschutzgesetz fachkundigen Datenschutzbeauftragten (DSB) bestellt?	☐ ja, interner DSB ☐ ja, externer DSB ☐ nein, der AN ist hierzu gesetzlich nicht verpflichtet ☐ nein	Wenn 6.1 ja: Nennen Sie bitten den Namen und Kontaktdaten Ihres DSB.	Name: _____ Telefonnummer: _____ E-Mailadresse: _____
6.2	Werden Ihre MA, die Auftragsdaten verarbeiten nachweislich im Datenschutzrecht geschult?	☐ ja, Präsenz-schulungen ☐ ja, eLearning ☐ nein	Wenn 6.2 nein: Wie stellen Sie sicher, dass Ihre MA, die Auftragsdaten verarbeiten, mit den Regeln des Datenschutzes vertraut sind?	☐ gar nicht ☐ Merkblätter
6.3	Werden Ihre MA nachweislich auf das Datenschutzgeheimnis nach § 5 BDSG verpflichtet?	☐ ja ☐ nein	keine	keine
6.4	Setzen Sie zur Erfüllung Ihrer Pflichten aus dem Vertrag mit dem AG auch Subunternehmer ein?	☐ ja ☐ nein	keine	keine
6.5	Sind die von Ihnen eingesetzten Subunternehmer im Vertrag mit dem AG oder von diesem gesondert schriftlich genehmigt?	☐ ja ☐ nein, bisher noch nicht	Wenn 6.5 Nein: Nehmen Sie bitte **umgehend** mit dem AG Kontakt auf, um die Tätigkeit der bisher nicht genehmigten Subunternehmer zu klären.	
6.6	Falls 6.4 ja: Wie stellen Sie sicher, dass Ihre Subunternehmer die Vorgaben dieses Vertrages mit dem AG und die Sie betreffenden Weisungen und Sicherheitsmaßnahmen umsetzen.	☐.Kein Prozess hierzu vorhanden ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer wurden bereits überprüft. Die Überprüfung wurde	keine	keine

	Mehrfachantworten möglich!!!	dokumentiert. Die Dokumentation wird dem AG zur Verfügung gestellt. ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer werden zeitnah überprüft. Die Überprüfung wird dokumentiert. Die Dokumentation wird dem AG zur Verfügung gestellt. ☐ Mit den Subunternehmern werden Verträge nach § 11 BDSG geschlossen. Diese können nach Aufforderung durch den AG diesem vorgelegt werden.		
6.7	Wurde Ihr Unternehmen bereits einmal von der für Sie zuständigen Aufsichtsbehörde für den Datenschutz überprüft?	☐ ja ☐ nein	Wenn 6.7 ja: Sind Sie in der Lage, den Prüfbericht samt Dokumentation der etwaig hiernach umgesetzten Maßnahmen dem AG vorzulegen.	☐ ja ☐ nein

7. Verfügbarkeitskontrolle

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
7.1	Verfügt der Serverraum über eine feuerfeste / feuerhemmende Zugangstür?	☐ ja ☐ nein	keine	keine
7.2	Ist der Serverraum mit Rauchmeldern ausgestattet?	☐ ja ☐ nein	keine	keine
7.3	Ist der Serverraum über eine Fernleitung an eine	☐ ja	keine	keine

	Brandmeldezentrale angeschlossen?	☐ nein		
7.4	Ist der Serverraum mit Löschsystemen ausgestattet? **Mehrfachantworten möglich!**	☐ ja, CO2 Löscher ☐ ja, Halon Löschanlage ☐ nein	keine	keine
7.5	Woraus bestehen die Außenwände des Serverraumes?	☐ Stein ☐ Ständerwände ☐ Beton	keine	keine
7.6	Ist der Serverraum klimatisiert?	☐ ja ☐ nein	keine	keine
7.7	Sind im Serverraum oder den Außenwänden des Serverraumes Wasserleitungen verlegt?	☐ ja ☐ nein	keine	keine
7.4	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)?	☐ ja ☐ nein	Wenn 7.4 ja: Wie lange gewährleistet die USV die Stromversorgung der Server?	☐ weniger als 10 Minuten ☐ weniger als 20 Minuten ☐ mehr als 20 Minuten
7.5	Verfügt der Serverraum zusätzlich über ein Dieselaggregat?	☐ ja ☐ nein	keine	keine
7.6	Existiert in Ihrem Unternehmen ein dokumentiertes Backup Konzept?	☐ ja ☐ nein	Wenn 7.6 ja: Sind Sie in der Lage, dem AG das Backup Konzept vorzulegen.	☐ ja ☐ nein
7.7	In welchen Rhythmus werden in Ihrem Unternehmen Backups der System angefertigt, auf denen die Auftragsdaten gespeichert werden.	☐ Echtzeitspiegelung ☐ täglich ☐ ein bis dreimal pro Woche ☐ seltener	keine	keine
7.8	Auf was für Sicherungsmedien werden die Backups gespeichert?	☐ Zweiter redundanter Server ☐ Sicherungsbänder ☐ Festplatten	keine	keine
7.9	Wo werden die Backups	☐ Zweiter redundanter Server steht an einem	Im Falle eines Transports der	☐ Mitnahme durch einen MA der IT /

	aufbewahrt / erstellt?	anderen Ort ☐ Safe, feuerfest, dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch ☐ Im Serverraum ☐ Privathaushalt	Backups: Wie wird dieser durchgeführt?	Geschäftsleitung / Sekretärin ☐ Abholung durch Bankmitarbeiter
7.10	Befindet sich der Aufbewahrungsort nach Ziff. 7.9 in einem vom Server aus betrachtet getrennten Brandabschnitt / Gebäudeteil?	☐ ja ☐ nein	keine	keine
7.11	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt?	ja, mittels stets aktualisiertem / -r ☐ Virenschutz ☐ Anti-Spyware ☐ Spamfilter ☐ Firewall		

8. Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Nr. 8 der Anlage zu § 9 Satz 1 BDSG).

☐ Nicht relevant = Trifft auf die konkrete Dienstleistung aufgrund der Art der Datenverarbeitung nicht zu.

Nr.	Frage:	Antwort	Folgefrage	Antwort
8.1	Wie sind die Auftragsdaten des AG von Daten anderer Kunden des AN getrennt?	☐ logische Trennung ☐ physische Trennung	keine	keine
8.2	Wie sind die Auftragsdaten des AG von eigenen Daten des AN getrennt?	☐ logische Trennung ☐ physische Trennung	keine	keine
8.3	Sind die zur Verarbeitung der Auftragsdaten eingesetzten Verfahren mandantenfähig?	☐ ja ☐ nein ☐ Es werden keine weiteren speziellen Verfahren eingesetzt, die Trennung erfolgt logisch auf Verzeichnisebene.	keine	keine

8.4	Existiert eine Dokumentation der Datenbank des AN, auf der die Auftragsdaten verarbeitet werden?	☐ ja ☐ nein	keine	keine
8.5	Existiert eine Dokumentation der Verfahren des AN, mit denen die Auftragsdaten verarbeitet werden?	☐ ja ☐ nein	keine	keine

Ort & Datum **Unterschrift des Auftragnehmer**

_____ _____

Hinweis:

Bei Änderungen der von Ihnen getroffenen und hier dokumentierten technischen – organisatorischen Sicherheitsmaßnahmen sind diese Änderungen dem Auftraggeber unverzüglich mitzuteilen. Dieser Anhang 2 ist dann entsprechend zu aktualisieren, mit dem aktuellen Tagesdatum zu versehen und von Ihnen zu unterschreiben und durch Abstimmung mit dem Auftraggeber unter Ersetzung der Vorversion zum neuen Vertragsbestandteil zu machen.