Sicherheitskonzept/ Datenschutzkonzept

Im Rahmen wissenschaftlicher Vorhaben bzw. klinischen Prüfungen werden Personen-/Probandendaten erfasst und verarbeitet. Bei diesen Daten handelt es sich gemäß Art. 9 Art. 1 DSGVO (siehe Kap. 3.4) um eine besondere Kategorie personenbezogener Daten, welche einen erhöhten Schutzbedarf aufweisen.
Das vorliegende Sicherheitskonzept beschreibt Maßnahmen zum Schutz der Verarbeitung besonderer Kategorien personenbezogener Daten im Kontext wissenschaftlicher Vorhaben bzw. klinischen Prüfungen an der Charité Universitätsmedizin Berlin.
Für die Verarbeitung personenbezogener Daten ist der Leiter des wissenschaftlichen Vorhabens / Leiter der klinischen Prüfung verantwortlich.
Datenschutzrechtliche Rahmenbedingungen:
Für die Charité - Universitätsmedizin Berlin gelten neben der Datenschutz-Grundverordnung (DSGVO) insbesondere landesrechtliche Regelungen wie das Landesdatenschutzgesetz (BlnDSG) und das Landeskrankenhausgesetz (LKG).

Zusammenfassung zum Studienprojekt:	*Die geplante Studie wird durchgeführt, um die positiven Versorgungseffekte - wie die Linderung der Symptomatik der kognitiven Beeinträchtigungen, Steigerung der Gesundheitskompetenz des Anwendenden, eine positive Beeinflussung der Lebensqualität, sowie eine gesteigerte Patient*innensouveränität - der mobilen Anwendung NeuroNation MED zu evaluieren. Die Applikation beinhaltet ein personalisiertes multi-domänen Gehirntraining zur Linderung der Symptome von Patient*innen mit leichten oder mäßigen kognitiven Beeinträchtigungen. Die Studie wird durchgeführt von der Forschungsgruppe Geriatrie der Charité –Universitätsmedizin Berlin, unter Leitung von Dr. Anika Heimann-Steinert, im Auftrag der Synaptikon GmbH. Ein zweites Zentrum ist das Gedächtniszentrum des UKJ Jena, das sich unter Leitung von Frau Prof. Dr. Kathrin Finke an der Studie beteiligt und dort spezifisch Patienten mit leichten kognitiven Defiziten nach Covid19-Infektionein schließt.*
Studientitel:	*Studie zur Evaluation einer mobilen Anwendung zum selbstständigen kognitiven Training - Effekte auf die kognitiven Fähigkeiten und die Lebensqualität von PatientInnen mit leichten kognitiven Störungen*

Kurztitel:	*NeuroNation MED Effektivitätsstudie (NeNaE)*
Studienleiter:	*Dr. Anika Heimann-Steinert*
Antragsnummer Ethikkommission:	*EA4/105//21*
Eudra CT Nr.:	-
ePA (des zentralen Studienregisters)	*Projektanzeige NeNaE: 20016499 (ePA)*
Studientyp	*Randomisierte kontrollierte Studie mit CE-gekennzeichneten Medizinprodukt, die im Rahmen der zugelassenen Zweckbestimmung eingesetzt wird*
Vorauss. Studienbeginn:	*01.06.2021*
Studienkoordinator	*Dr. Anika Heimann-Steinert*
Studienärzte:	-
Betroffene der Datenverarbeitung	● PatientInnen mit leichten kognitiven Einschränkungen (insbesondere mit der Diagnose F07.1, F06.7., F07.2, F06.8)
Externe Beteiligte/ Auftragsverarbeiter/ Weitergabe von Daten an Dritte und Schutzmaßnahmen	● *Daten werden vom Gedächtniszentrum des UKJ Jena aufgenommen und an die Charité postalisch versendet* ● *Daten werden an die Synaptikon GmbH und an das Gedächtniszentrum des UKJ Jena nur anonymisiert weitergegeben* ● *Es besteht eine Kooperationsvereinbarung mit folgenden externen Beteiligten:* - *Gedächtniszentrum des UKJ Jena* - *Synaptikon GmbH*
Weitergabe von Daten oder Proben in EU-/ Nicht EU Ausland	*Nicht zutreffend.*
Auftragskontrolle	*Eine Auftragsdatenverarbeitung findet im Zusammenhang mit der durchzuführenden Studie nicht statt. Multizentrisch: Joint Controllership. Des Weiteren werden lediglich anonymisierte Daten mit dem Kooperationspartner Synaptikon GmbH verarbeitet. Der Kooperationsvertrag legt als Vertragswerk, die Rechte und Pflichten fest.*
Beschreibung des Dokumentationsverfahrens	*Gegenstand der Studie ist die Erhebung der kognitiven Fähigkeiten von NutzerInnen mit der Diagnose F06.7 zur Untersuchung der Wirksamkeit und Effektivität des Trainingsprogrammes.* *Zusätzlich soll der Einfluss des Trainingsprogrammes auf die soziale Teilhabe, Depressivität und Gesundheitsbezogene Lebensqualität von NutzerInnen mit der Diagnose F06.7 erhoben werden. Des Weiteren findet*

	eine Ermittlung der Gebrauchstauglichkeit und des Anwendungserlebnisses für die Nutzergruppe mit der Diagnose F06.7 statt. *Die erhobenen Daten aus dem einleitenden Fragebögen werden in Papierform erfasst und entsprechend im ISF abgelegt. Weitere Notizen werden im Rahmen der Datensicherung auf Papier protokolliert und später digital verschriftlicht. Weitere Notizen werden im Rahmen der Datensicherung auf Papier protokolliert.* *Die entsprechende Datenablage erfolgt in einem abgesicherten Ordner innerhalb des Netzwerkes der Charité. Dieser Ordner ist ausschließlich für die Mitglieder der Arbeitsgruppe zugänglich. Weitere Zugriffsmöglichkeiten bedürfen der aktiven Freischaltung durch den Rechteinhaber des Ordners (FGG). Die Zugriffsrechte innerhalb des Studienteams sind durch den Studienleiter geregelt, jede Änderung dieser Rechte bedarf dessen Zustimmung.* *Darüber hinaus erfolgt die Löschung der Studiendaten nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist von 10 Jahren.* *Die probandenbezogenen Daten werden in pseudonymisierter Form erfasst. Jeder Proband ist durch eine zwei. Probandennummer, zugewiesen bei der Registrierung, unverwechselbar gekennzeichnet. Der Studienleiter führt eine vertrauliche Probandenliste, in der die Kenndaten mit dem vollen Probandennamen verbunden sind, in die nur er und ein weiteres Mitglied des Studienpersonals Einsicht hat. Die Fragebögen werden in einem abschließbaren Schrank im Studienzentrum aufbewahrt.* ● *Zusammensetzung der Probandennr.: zufällig* ● *Papier-CRF* ● *geschützter Serverbereich:* *\\Charite.de\Centren\C13\WER\#WER-Public\Alter-und-Technik\FGG_49_NeuroNation* ● *Zugriff auf Studiendokumentation hat das Studienpersonal der Charité – Forschungsgruppe Geriatrie* ● *Zugang zu Server durch autorisierte Personen entspr. Zugriffsrechte:* ● *Die Studienunterlagen werden als Teil der Studienakte ausgedruckt*

Papierdaten	● *Aufbewahrungsort Patientenakte, Studienakte, CRF: Räumlichkeiten der Forschungsgruppe Geriatrie – AG Alter und Technik Reinickendorfer Str. 61 13347 Berlin* ● *Zugriffsbeschränkter Raum, abschließbare Schränke* ● *Eine Rückverfolgung der Daten des CRF zu einem Patienten ist ohne Identifizierungsliste nicht möglich.* ● *Auf die Identifizierungsliste haben nur der Studienleiter Zugriff.*
Datenbank	● *Im Rahmen der Studie werden Daten in der Datenbank im Studienzentrum gespeichert. Die Login-Daten der App werden anonymisiert auf die Server von Amazon Web Services EMEA SARL ("AWS Europe") transferiert. Eine ausführliche Erklärung in Bezug auf die Datensicherheit liegt als separates Schreiben bei.*
App oder weitere technische Besonderheiten	*Verwendung der NeuroNation MED-App*
Archivierung:	*Gemäß den gesetzl. Vorgaben (s. ZVA: Aufgaben und Pflichten der Sponsorvertretung, Kap. 3.4.6)* *Archiviert wird durch die Charité in den Räumlichkeiten der Forschungsgruppe Geriatrie – AG Alter und Technik Reinickendorfer Str. 61 13347 Berlin. Der Sponsor stellt sicher, dass die wesentlichen Unterlagen der klinischen Prüfung einschließlich der Prüfbögen nach der Beendigung oder dem Abbruch der Prüfung mindestens zehn Jahre aufbewahrt werden.*
Veröffentlichung von Daten	● *Es erfolgt keine Veröffentlichung von Daten in nicht-anonymisierter Form.* ● *Daten werden in anonymer Form auf medizinischen Kongressen präsentiert.* ● *Artikel in med. Fachliteratur*
folgende Daten werden erhoben/ Datenkategorien	● *Nutzer-ID* ● *Visit-Datum* ● *Name* ● *Vorname* ● *Alter* ● *Geschlecht* ● *Anschrift* ● *E-Mail-Adresse* ● *Familienstand* ● *Bildungsgrad* ● *Erkrankungen* ● *Medikation* ● *Sportliche Aktivität* ● *(App-)Nutzungsdaten:*

	○ *userId,* ○ *exerciseId,* ○ *timestamp* ○ *score* ○ *startDifficulty* ○ *endDifficulty* ○ *meanDifficulty* ○ *minDifficulty* ○ *maxDifficulty* ○ *avgBadReactionTime* ○ *avgGoodReactionTime* ○ *Accuracy* ● *Fragebogen-/Assessmentdaten*
Allgemeine organisatorische Maßnahmen	● *Jeder Mitarbeiter des Studienteams wird bei der Aufnahme seiner Tätigkeit schriftlich und mündlich auf das Datengeheimnis bzw. das Einhalten der Schweigepflicht sowie auf das Einhalten entsprechender interner Richtlinie verpflichtet. Insbesondere wird die unbefugte Weitergabe von Daten an Dritte und das Verbringen schutzwürdiger Daten nach außen verboten.* ● *Die potentiellen Teilnehmer werden sowohl in der Studieninformation und Einwilligungserklärung als auch im Rahmen des Aufklärungsgesprächs über die Einhaltung des Datenschutzes, Art und Umfang der gespeicherten Daten, die Weitergabe von Daten und das Recht an den eigenen Daten (inkl. Auskunft, Berichtigung, Einschränkung der Verarbeitung, Widerruf und Löschung) informiert* ● *Betroffene Personen können sich jederzeit an die für die Datenerhebung und Verarbeitung verantwortlichen Stellen wenden. Entsprechende Kontaktdaten sind sowohl in der Studieninformation als auch in der Einwilligungserklärung aufgeführt.*
Technisch organisatorische Maßnahmen (Ausführungen s. Kap. 6)	● *Pseudonymisierung von Daten im CRF (Excel)* ● *Zutrittskontrolle zu den Räumlichkeiten (betrifft Büros zur Aufbewahrung von Unterlagen in Papier) ist nur autorisierten Personen möglich und wird durch eine Schlüsselvergabe geregelt* ● *Zur Therapie gehören neben der Nutzung der App auch psychoedukative Materialien, die den TeilnehmerInnen von Seiten des Herstellers per Mail zugesandt werden. Um die persönlichen Daten der NutzerInen zu schützen und um insbesondere eine Weitergabe der Kontakt-Mailadressen außerhalb der Charité zu vermeiden, wird von Seiten der Charité ein Verteiler*

	angelegt, in dem die Adressen der ProbandInnen hinterlegt sind. Der App-Hersteller hat darauf keinen Zugriff und sendet die Materialien lediglich zu dem allgemeinen Verteiler und hat keine Einsicht auf die sich dahinter verbergenden Mailadressen.
	● *Zugriff zu studienspezifischen elektronische Dateien: PC Arbeitsplätze der Charité, Server-Infrastruktur, Berechtigungssystem, passwortgeschützter Zugang zum persönl. Charité Account*
	● *Datenübertragung Charité intern in pseudonymisierter Form und extern in anonymisierter Form*
	● *regelmäßige automatische Sicherung der Studiendaten erfolgt routinemäßig über den GB IT*
	
	● *Bei der Verwaltung der digitalen Gesundheitsanwendung NeuroNation MED wird die Amazon Web Services EMEA SARL ("AWS Europe") als Dienstleister angeführt. Ein Datenfluss von personenbezogen Daten in die USA kann hierbei aufgrund technischer und organisatorischer Maßnahmen vollumfassend ausgeschlossen werden. Dies begründet sich durch Folgendes:*
	  ● *Die Synaptikon GmbH ist der exklusive und juristische Besitzer der Schlüssel, mit denen personenbezogene Daten verschlüsselt werden*
	  ● *Die Schlüssel werden im Rechenzentrum unseres Dienstleisters in Deutschland zur Verschlüsselung automatisch angewendet und ausschließlich durch die Synaptikon GmbH administriert*
	  ● *Technische und organisatorische Maßnahmen schließen aus, dass der Dienstleister die Schlüssel lesen oder in andere Rechenzentren außerhalb Deutschlands verschieben kann.*

Gesetzliche Rahmenbedingungen und Definitionen

Inhalt

1. Definitionen

1.1. Verarbeitung (i.S. Art. 4 Abs. 2 DSGVO)

[…] jede(r) mit oder ohne Hilfe automatisierter Verfahren ausgeführte(r) Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

1.2. Verantwortlicher (i.S. Art. 4 Abs. 7 DSGVO)

[…] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

1.3. Personenbezogene Daten (i.S. Art. 4 DSGVO)

[…] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

1.4. Besondere Kategorie personenbezogener Daten (i.S. Art. 9 DSGVO)

[…] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person […]

1.5. Betroffene Person

[…] jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten von dem für die Verarbeitung Verantwortlichen verarbeitet werden.

2. Verantwortliche Stelle im Sinne des Datenschutzes an der Charité

Die Verantwortung für die Sicherheit der Daten und für eine ordnungsgemäße Datenverarbeitung liegt beim Vorstand der Charité und dem Leiter des wissenschaftlichen Vorhabens/Prüfer der klinischen Prüfungen.
Spezifische Anliegen erfordern ferner die Hinzunahme des Geschäftsbereiches Datenschutz und Governance der Charité Universitätsmedizin Berlin. Dieser muss bei folgenden Anliegen zusätzlich konsultiert werden:

- Beschwerden den Datenschutz betreffend
- Datenschutzprobleme
- Auskunftsgesuch der betroffenen Person (gemäß Art. 15 DSGVO)
- Anfragen von Datenschutz-Aufsichtsbehörden (gemäß Art. 58 DSGVO)

3. Grundsätze der Datenverarbeitung

Die Verarbeitung personenbezogener Daten unterliegt spezifischen Grundsätzen. Im Kontext von wissenschaftlichen Vorhaben und klinischen Prüfungen gelten insbesondere:

3.1. Verarbeitung personenbezogener Daten (gemäß Art. 5 DSGVO)

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (i.S. Art. 5 Abs 1 lit a DSGVO)
    - Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

- Zweckbindung (i.S. Art. 5 Abs 1 lit b und Art. 9 DSGVO)
    - Daten dürfen ausschließlich für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden
    - Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt (gemäß Artikel 89 Abs. 1 DSGVO) nicht als unvereinbar mit den ursprünglichen Zwecken
    - Es ist ausdrücklich zu beachten, dass bei der Verarbeitung von Gesundheitsdaten zusätzlich Art. 9 DSGVO gilt (siehe Kapitel 5.3).

- Datenminimierung ((i.S. Art. 5 Abs 1 lit c DSGVO)
    - Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein

- Richtigkeit (i.S. Art. 5 Abs 1 lit d DSGVO)
    - Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten 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

- Speicherbegrenzung (i.S. Art. 5 Abs 1 lit e DSGVO)
    - Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
    - Personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, verarbeitet werden

- Integrität und Vertraulichkeit (i.S. Art. 5 Abs 1 lit f DSGVO)
    - Daten müssen 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

- Rechenschaftspflicht (i.S. Art. 5 Abs. 2 DSGVO)
    - Für die Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DSGVO ist der Verantwortliche zuständig. Die Erfüllung muss der Verantwortliche nachweisen können.

3.2. Rechtmäßigkeit der Verarbeitung (gemäß Art. 6 und Art. 9 DSGVO)

Die Datenverarbeitung im Sinne der DSGVO unterliegt besonderen Bedingungen. Ohne die Erfüllung einer dieser Voraussetzungen, gilt die Verarbeitung als nicht rechtmäßig. Eine der nachfolgenden Voraussetzungen muss mindestens vorliegen:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben […] (gemäß Art. 6 Abs. 1 lit a DSGVO)
- die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen […] (gemäß Art. 6 Abs. 1 lit b DSGVO)
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt […] (gemäß Art. 6 Abs. 1 lit c DSGVO) – bspw. die Meldung/Dokumentation über das Krebsregister
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen […] (gemäß Art. 6 Abs. 1 lit d DSGVO)
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde […] (gemäß Art. 6 Abs. 1 lit e DSGVO)

Es ist ausdrücklich zu beachten, dass Im Kontext wissenschaftlicher Vorhaben / klinischen Prüfungen **zusätzlich** Art. 9 DSGVO gilt (siehe Kapitel 5.3).

3.3. Verarbeitung besonderer Kategorien personenbezogener Daten (gemäß Art. 9 DSGVO)

Die Verarbeitung von Daten dieser Kategorie sind untersagt (Art. 9 Abs. 1 DSGVO). Im der klinischen Forschung machen nachfolgende Bedingungen eine Datenverarbeitung hingegen möglich:

- (d)ie betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden (i.S. Art. 9 Abs. 2 lit a)
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben […] (i.S. Art. 9 Abs. 2 lit c)
- die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 (gemäß Art. 9 DSGVO) genannten Bedingungen und Garantien erforderlich […] (i.S. Art. 9 Abs. 2 lit h)
- die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich […] […] (i.S. Art. 9 Abs. 2 lit i)

4. Rechte der Betroffenen (gemäß Kap. 3 Art. 12 -23 DSGVO)

Im Rahmen des wissenschaftlichen Vorhabens / der klinischen Prüfung sind die Rechte der Betroffenen besonders zu wahren. Dazu zählen insbesondere:

- Recht auf Auskunft zu personenbezogenen Daten (i.S. Art. 15 DSGVO)
    - Die betroffene Person hat gegenüber dem Verantwortlichen einen Recht auf Auskunft darüber, welche Daten zu ihrer Person gespeichert werden, zu welchem Zweck die Daten gespeichert werden sowie über die Empfänger und die Herkunft der Daten. Der Verantwortliche ist in der Pflicht, wahrheitsgemäße Angaben zu tätigen. Die Auskunft muss vollständig sein und alle verarbeiteten Daten erfassen.
- Recht auf Berichtigung (i.S. Art. 16 DSGVO)
    - Wurden personenbezogenen Daten unrichtig erhoben, hat die betroffene Person ein Recht auf Berichtigung der entsprechenden Daten. Unter Berücksichtigung des Verarbeitungszweckes hat die betroffene Person ebenso das Recht auf Vervollständigung seiner bereits verbreiteten Daten. Auf Verlangen ist dem unverzüglich Folge zu leisten.
- Recht auf Löschung / Recht auf „Vergessenwerden“ (i.S. Art. 17 DSGVO)
    - Die betroffene Person hat das Recht die Löschung seiner betreffenden personen-bezogenen Daten zu verlangen. Der Verantwortliche ist verpflichtet, die Löschung unter Berücksichtigung der Existenz einer der nachfolgenden Bedingungen, unverzüglich vorzunehmen:
        - Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
        - Die betroffene Person widerruft ihre Einwilligung. (Anmerkung: Im Rahmen eines wissenschaftlichen Vorhabens / einer klinischen Prüfung dürfen die **bis zum Widerruf bereits verarbeiteten Daten** für Studienzwecke weiterverwendet werden (gemäß Art. 7 Abs. 3 DSGVO).
        - Die betroffene Person erhebt Widerspruch gegen die Verarbeitung und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
        - Die personenbezogenen Daten der betroffenen Person wurden unrechtmäßig erhoben.
- Recht auf Einschränkung der Verarbeitung (i.S. Art. 18 DSGVO)
    - Unter Voraussetzung einer der nachfolgenden Bedingungen hat die betroffene Person das Recht, die Einschränkung der Verarbeitung seiner betreffenden personenbezogenen Daten zu verlangen:
        - Die Richtigkeit der Verarbeitung personenbezogenen Daten wird von der betroffenen Person bestritten.
        - Der Verarbeitung personenbezogener Daten ist unrechtmäßig, die betroffene Person lehnt jedoch die Löschung seiner betroffenen Daten ab und fordert die Einschränkung der Nutzung seiner personenbezogenen Daten
        - Die personenbezogenen Daten werden für den ursprünglichen Verarbeitungszweck nicht länger benötigt, die betroffene benötigt diese jedoch hinsichtlich der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen.
        - De betroffene Person hat Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten eingelegt und es ist noch unklar, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen
    - Wurden personenbezogene Daten in ihrer Verarbeitung eingeschränkt, dürfen diese einzig unter der Voraussetzung einer der nachfolgenden Bedingungen erneut verarbeitet werden:
        - Einwilligung der betroffenen Person
        - Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
        - Schutz der Rechte einer anderen natürlichen oder juristischen Person

        - Gründe eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaates
- Recht auf Datenübertragbarkeit (i.S. Art. 20 DSGVO)
    - Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und bei Bedarf mit einem anderen Verantwortlichen zu teilen.
    - Unter Voraussetzung der technischen Möglichkeiten hat die betroffene Person das Recht eine Übermittlung der personenbezogenen Daten von einem Verantwortlichen zu einem anderen Verantwortlichen zu erwirken.
- Recht auf Widerspruch (i.S. Art. 21 DSGVO)
    - Die betroffene Person jederzeit hat das Recht, die Verarbeitung seiner personenbezogenen Daten zu widersprechen. Der Verantwortliche muss die Verarbeitung unverzüglich einstellen, sofern nicht eine der nachfolgenden Bedingungen dem entgegensteht:
        - Nachweis zwingend schutzwürdiger Gründe
        - Interessen, Rechte und Freiheiten der betroffenen Person überwiegen
        - Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Nach Art. 89 DSGVO können von den o.g. Rechten gemäß der Artikel 15, 16, 18 und 21 Ausnahmen vorgesehen werden, wenn personenbezogene Daten zu wissenschaftlichen Zwecken verarbeitet werden und diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

So sieht Art. 17 Abs. 3 c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit sowie Art. 17 Abs. 3 d) DSGVO für wissenschaftliche Forschung eine Ausnahme von dem Recht auf Löschung vor, wenn die Verwirklichung die Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.
Außerdem beschränkt § 17 (4) des Berliner Datenschutzgesetzes die Rechte der betroffenen Person insoweit, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 DSGVO besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.
Gemäß Art. 7 Abs. 3 DSGVO haben Betroffene ferner die Möglichkeit und das Recht, ihre Einwilligung zur Datenverarbeitung zu widerrufen. Im Rahmen eines wissenschaftlichen Vorhabens / einer klinischen Prüfung, dürfen die bis zum Widerruf bereits verarbeiteten Daten für Studienzwecke weiter verwendet werden.

5. Art der zu verarbeitenden Daten

Bei den betroffenen Personen handelt es sich um Teilnehmer im Kontext wissenschaftlicher Vorhaben / klinischer Prüfungen.
Alle im Rahmen des wissenschaftlichen Vorhabens/klinischen Prüfungen erhobenen Daten sind Studiendaten. Ihre Verwendung erfolgt zum Zwecke der Erreichung der entsprechenden Ziele des Vorhabens/der klinischen Prüfung. Verarbeitungszweck und Ziele sind im Ethikantrag/Prüfplan entsprechend formuliert und begründet. Die Verarbeitung von personenbezogenen Daten ist einzig im Kontext des Prüfplans bzw. des Ethikantrages sowie den entsprechenden Gesetzesnormen (Art. 5 DSGVO und Art. 6 Abs. 1 DSGVO) gestattet.

Studiendaten sind persönliche Informationen des Teilnehmers (z.B. Name, Geburtsdatum, Adresse und Daten zur Gesundheit bzw. Erkrankung). Darüber hinaus werden Daten, die aus der während der wissenschaftlichen Untersuchung/klinischen Prüfung gemäß Prüfplan durchgeführten Diagnostik und Behandlung resultieren, verarbeitet. Die Datenverarbeitung erfolgt entsprechend den im Ethikantrag/Prüfplan getätigten Angaben.

6. Technisch-Organisatorische Maßnahmen

Entsprechend den datenschutzrechtlichen Bestimmungen sind Maßnahmen zu treffen, die gewährleisten, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

6.1. Maßnahmen zur Sicherung der Vertraulichkeit

Es muss gewährleistet werden, das unbefugte Personen keinen Zugang zu den entsprechenden Daten erhalten.

6.1.1. Pseudonymisierung

Unter dem Begriff Pseudonymisierung versteht man die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Voraussetzung ist jedoch, dass diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Pseudonyme müssen zusammen mit den identifizierenden Eigenschaften einer Person in einer separaten Teilnehmeridentifikationsliste geführt und in einem getrennten und abgesicherten Systemen aufbewahrt werden (bestenfalls verschlüsselt).
Die Dokumentation von personenbezogenen Daten zu erfolgten Therapien (den sog. Quelldaten) findet in der Patientenakte unter dem realen Namen des Teilnehmers statt. Die im Ethikantrag aufgeführten bzw. vom Prüfplan geforderten Informationen müssen pseudonymisiert in ein studienspezifisches CRF überführt werden. Dieses kann sowohl papierbasiert als auch elektronisch sein. Bei einer elektronischen Verarbeitung muss darauf geachtet werden, das einzig pseudonymisierte Daten exportiert werden. Bildhafte Befunde (MRT) sowie entnommene Biomaterialien müssen ebenfalls pseudonymisiert abgespeichert werden und dürfen einzig in dieser Form Verwendung finden.

6.1.2. Zutrittskontrolle

Die Zutrittskontrolle soll gewährleisten, das Unbefugten der Zutritt zu Datenverarbeitungsanlagen bzw. Räumen, in denen personenbezogene Daten verarbeitet werden, verwehrt wird.
Der Zutritt zu den Räumlichkeiten (Büros zur Aufbewahrung von Unterlagen in Papier sowie Laborräume zur Lagerung von Biomaterialien) ist nur autorisierten Personen möglich. Dies wird durch

eine kontrollierte Transponder- bzw. Schlüsselvergabe sichergestellt. Sowohl Transponder als auch Schlüssel dürfen NICHT an nicht-autorisierte Personen weitergegeben werden. Zimmertüren sind von der letzten Person, die einen Raum verlässt, abzuschließen. Beim Ausscheiden eines Mitarbeiters hat dieser sowohl den Transponder als auch empfangene Schlüssel unverzüglich zurückzugeben. Die Vergabe von Transponder und Schlüssel ist zu dokumentieren.

6.1.3. Zugangskontrolle und Zugriffskontrolle

Die Zugangskontrolle soll sicherstellen, dass einzig die dazu berechtigten Personen Zugang zu den Datenverarbeitungssystemen erhalten. Mit Hilfe der Zugriffskontrolle muss gewährleistet werden, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen einzig 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.

Auf Papier dokumentierte personenbezogene Daten (bspw. Einwilligungserklärungen, Patienten- und Probandenakten) müssen in verschließbaren Schränken aufbewahrt werden. Die Schlüsselvergabe ist innerhalb des Studienteams zu organisieren und zu kontrollieren. Die Schlüsselvergabe ist zu dokumentieren. Eine kontrollierte Schlüsselvergabe soll sicherstellen, dass nur autorisierte Mitarbeiter des Studienteams Zugriff auf die Daten haben. Schlüssel dürfen NICHT an nicht-autorisierte Personen weitergegeben werden. Die Schränke sind stets verschlossen zu halten. Beim Ausscheiden eines Mitarbeiters muss der entsprechende Schlüssel unverzüglich zurückzugeben werden.

Daten, welche systembasiert verarbeitet werden auf einem Datenbankserver gespeichert. Der Datenbankserver muss sich in der Charité-DMZ befinden. Der Systemzugriff erfolgt über einen persönlichen Benutzeraccount. Kooperationspartner erhalten ggf. nach schriftlicher Genehmigung durch den Studienleiter Systemzugriff. Die Zugriffslaufzeit ist dabei auf die Projektdauer beschränkt. Geeignete Garantien und Vereinbarungen zur ordnungsgemäßen Nutzung von personenbezogenen Daten sind vertraglich festzuhalten und schriftlich zu bestätigen.

Die Dateneingabe muss im gesicherten Netz der Charité – Universitätsmedizin Berlin erfolgen und ist durch ein Berechtigungskonzept geregelt. Für die Dateneingabe ist der persönliche Benutzeraccount zu verwenden. Eine Dateneingabe unter Verwendung eines fremden Benutzeraccounts ist nicht zulässig und strengstens untersagt. Über den Benutzeraccount sind die entsprechen Berechtigungen innerhalb des Studienprojektes geregelt. Nach einer längeren Inaktivität wird der Benutzer automatisch ausgeloggt. Ein standardisiertes Passwortverfahren soll die Zusammensetzung einzelner Komponenten regeln.

Elektronische Daten dürfen einzig innerhalb der in der Verantwortung des GB IT stehenden Serverinfrastruktur gespeichert werden. Dabei muss der verfügbare Ordner der Arbeitsgruppe verwendet werden. Der Zugang ist nur autorisierten Mitarbeitern der AG möglich. Die Berechtigung wird im Auftrag und nach Bestätigung des Leiters der AG durch den GB IT freigegeben. Die Freigabe von Berechtigungen wird dokumentiert. Der Zugang auf die Server-Infrastruktur erfolgt passwortgeschützt unter Verwendung des persönlichen Charité-Account. Nach Beendigung der Arbeit muss ein Logout durch den Benutzer erfolgen, um einen Zugriff Unbefugter zu vermeiden.

Elektronisch geführte Teilnehmeridentifikationslisten sind durch ein Passwort zu sichern. Für das Generieren des Passwortes werden die Ausführungen des zentral gelenkten QM-Dokuments „Kennwortrichtlinie der Charité“ berücksichtigt. Autorisierte Mitarbeiter des Studienteams erhalten im Rahmen einer persönlichen Einweisung das Passwort der Teilnehmeridentifikationsliste mitgeteilt. Die Mitteilung des Passwortes muss dokumentiert werden. Es muss regelmäßig auf den ordnungsgemäßen Umgang mit der Datei sowie mit deren Passwort hingewiesen.

Ein Speichern von personenbezogenen Daten auf privaten Endgeräten und/oder über Cloud Computing ist nicht zulässig.

6.1.4. Trennungskontrolle

Unter die Trennungskontrolle fallen alle Maßnahmen, die gewährleisten, das Daten getrennt voneinander verarbeitet werden können. Erreicht wird das in der Regel durch eine logische und physikalische Trennung der Daten.
Die identifizierenden Daten der Teilnehmer (Name, Geburtsdatum und Kontaktdaten), anhand dessen ein eindeutiger Bezug zur betroffenen Person hergestellt werden könnte, müssen getrennt von den Studiendaten in einer Teilnehmeridentifikationsliste aufbewahrt werden. Rückschlüsse auf einzelne Teilnehmer einzig mit Hilfe der Teilnehmeridentifikationsliste möglich. Sie darf einzig autorisierten Mitarbeitern des Studienteams zugänglich sein. Dieser Umstand gilt sowohl während als auch nach Abschluss des wissenschaftlichen Vorhabens/klinischen Prüfung. Im Fall schwerwiegender Begleitumstände während des Vorhabens, muss eine Re-Pseudonymisierung möglich sein.
Im Falle einer systembasierten Datenverarbeitung muss sichergestellt werden, dass die Anwendung zwei Umgebungen unterscheidet. Eine Entwicklungsumgebung, zur Erstellung, Modifikation und Löschung von Formularen/eCRFs. Daneben muss eine Produktionsumgebung bestehen, in welcher letztlich die realen Daten verarbeitet werden. In der Produktionsumgebung ist eine Modifikation und Löschung der Formulare/eCRFs nicht möglich. Ferner muss ein Berechtigungskonzept die jeweiligen Nutzerrechte bzgl. der Datenverarbeitung im System bzw. Studienprojekt entsprechend regeln.

6.2. Maßnahmen zur Sicherung der Integrität

Es muss gewährleistet werden, dass die Daten während der Verarbeitung nicht von Unbefugten modifiziert werden können.

6.2.1. Weitergabekontrolle

Bei der Weitergabekontrolle handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Daten dürfen sowohl intern einzig in anonymisierter bzw. pseudonymisierter Form weitergegeben werden. Klarnamen und identifizierende Merkmale sind zu vermeiden. Es muss darauf geachtet werden, dass eine Datenverarbeitung stets über eine verschlüsselte Verbindung (bspw. https) oder unter Einsatz eines VPN-Zugriffs erfolgt. Darüber hinaus sollte die Weitergabe relevante Inhalte per E-Mail unter Einsatz von Verschlüsselungs- und Signaturmechanismen erfolgen.
Auf Grund der Komplexität im Hinblick auf eine externe Weitergabe sei an dieser Stelle auf Kapitel 3 der DSGVO verwiesen. Im Zweifel ist der Datenschutzbeauftragte zu konsultieren.

6.2.2. Eingabekontrolle

Unter Eingabekontrollen sind Maßnahmen zu verstehen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrollen (sog. Audit Trail) können auf unterschiedlichen Ebenen (bspw. Betriebssystem, Datenbank, Anwendung) stattfinden.
Die verarbeiteten Daten müssen regelmäßig auf Plausibilität und Vollständigkeit überprüft und gegebenenfalls korrigiert und/oder ergänzt werden. Im Rahmen eines geplanten Monitorings müssen die Quelldaten aus der Patienten- bzw. Probandenakte mit den Eintragungen im CRF abgeglichen werden. Bei festgestellten Mängeln muss eine Korrektur erfolgen, welche ebenfalls zu dokumentieren ist. Dies gilt sowohl für die papierbasierte als auch die elektronische Form der Datenverarbeitung.
Im Rahmen einer systembasierten Datenverarbeitung können die entsprechenden Nutzerrechte hinsichtlich der Eingabe, der Änderung und der Löschung von Daten bzw. Dateneingaben geregelt werden.

6.3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

6.3.1. Verfügbarkeitskontrolle

Hierbei handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Eine zyklische Datensicherung muss über ein Backup-Konzept geregelt sein. Die daraus resultierenden Sicherungen müssen getrennt und außerhalb des Serverraumes aufbewahrt werden. Daneben muss sichergestellt werden, dass die Sicherungsmedien eine korrekte Wiederherstellung der Daten erlauben. Es müssen regelmäßige Tests und Protokollierungen stattfinden, um den korrekt funktionierende Wiederherstellungsvorgang zu bestätigen bzw. nachweisen zu können. Dieser Prozess muss in einem Recoverykonzept geregelt sein.
Personenbezogene Daten müssen so lange aufbewahrt werden, wie dies im Rahmen eines wissen-schaftlichen Vorhabens/einer klinischen Prüfung gesetzlich vorgeschrieben ist und/oder nach den Empfehlungen zur Sicherung guter wissenschaftlicher Praxis notwendig erscheint. Nicht mehr benötigte Daten müssen durch sicheres Überschreiben / endgültiges Löschen der Datensätze und Entfernen etwaiger Sicherheitskopien gelöscht werden. Vorhandene und nicht mehr benötigte Proben komplett vernichtet werden.
Ist eine Löschung nicht vorgesehen und/oder nicht möglich, müssen die vorhandenen Studiendaten anonymisiert werden. Bei einer Anonymisierung werden die personenbezogenen Daten derart verändert, dass ein Rückschluss auf die Betroffenen wesentlich erschwert wird bzw. Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Vorgänge zur Löschung, Vernichtung oder Anonymisierung müssen dokumentiert werden.

6.4. Maßnahmen zur Sicherung der Authentizität

Studiendaten müssen sich ihrem Ursprung anhand von Quelldaten in der Patienten- bzw. Probandenakte zuordnen lassen.

6.5. Maßnahmen zur Sicherung der Revisionsfähigkeit und Transparenz

Eintragungen, Änderungen und Streichungen müssen im Rahmen der papierbasierten Verarbeitung mit einem persönlichen Namenskürzel sowie dem aktuellen Datum versehen werden. Bei einer elektronischen Verarbeitung muss dies der Audit Trail gewährleisten.

6.6. Datenschutzfreundliche Voreinstellungen (Privacy by design / Privacy by default)

6.7. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Zur Überprüfung der Wirksamkeit der festgelegten Maßnahmen soll regelmäßig erfolgen. Zu berücksichtigen sind eine regelmäßige Bewertung der mit den Verarbeitungstätigkeiten einhergehenden Risiken für die betroffenen Personen (projektbezogene Risikoanalysen und Datenschutzfolgeabschätzungen). Dokumentierte Datenschutzvorfälle werden entsprechend berücksichtigt.