GUIDE

Leitlinien für den Datenschutz in der wissenschaftlichen Forschung zu Aspekten der Mensch-Technik-Interaktion

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Fraunhofer
IOSB

FH Bielefeld
University of
Applied Sciences

Inhaltsverzeichnis

1. Einleitung

Die Europäische Datenschutz-Grundverordnung und ihre Bedeutung für deutsche Forschungsprojekte zu Aspekten der Mensch-Technik-Interaktion (GUIDE)

Das Forschungsprojekt „Die Europäische Datenschutz-Grundverordnung und ihre Bedeutung für deutsche Forschungsprojekte zu Aspekten der Mensch-Technik-Interaktion (GUIDE)“ startete zum 01.10.2017. Forschungsziel war es, die Europäische Datenschutz-Grundverordnung (DSGVO) und ihre Bedeutung für Forschungsprojekte der Mensch-Technik-Interaktion zu untersuchen. Dazu hat sich ein interdisziplinäres Konsortium aus Juristen und Technikern in enger Abstimmung mit dem vom BMBF beauftragten Projektträger VDI/VDE Innovation + Technik GmbH zusammengefunden. Hauptsächlich am Projekt beteiligt waren Frau Prof. Dr. Steckler von der Fachhochschule Bielefeld und Dr.-Ing. Erik Krempel vom Fraunhofer IOSB Karlsruhe.

a. Der Begriff Datenschutz

Im deutschen Sprachraum werden die Begriffe „Datenschutz“ und „Datensicherheit“ oft als Synonyme verwendet, obwohl sie unterschiedliche Bedeutungen haben. Datenschutz bezeichnet das Bestreben, bei der Verarbeitung personenbezogener Daten die Rechte und Freiheiten natürlicher Personen zu wahren. Mögliche Risiken für diese Rechte und Freiheiten, insbesondere im Rahmen von der Datenverarbeitung in Forschungsprojekten können dabei sein:

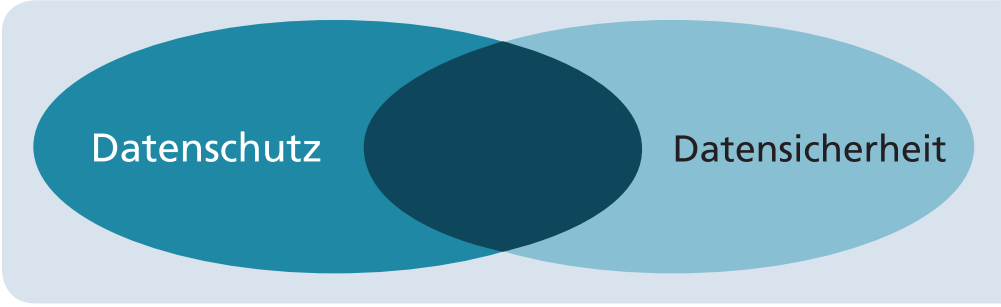
- Verletzung der Menschenwürde (Art. 1 GG)
- Verletzung des Allgemeinen Persönlichkeitsrechts (Art. 2 GG)
- Verletzung besonderer Persönlichkeitsrechte, z.B. das Recht am eigenen Bild
- Körperverletzung, z.B. infolge fehlerhafter Gesundheitsdaten
- Sachschäden, z.B. infolge unzutreffender Daten
- Finanzieller Verlust
- Rufschädigung
- Diskriminierung

Je nach Forschungsfeld kommen unterschiedliche Datenschutzgesetze zur Anwendung, in der gesamten EU genießt aber die DSGVO (Anwendungs-)Vorrang vor allen anderen. In deutschen Forschungsprojekten sind das Bundesdatenschutzgesetz (BDSG) und weitere bereichsbezogene Datenschutzgesetze einschlägig.

Der Begriff Datensicherheit hingegen wird zwar im alltäglichen Gebrauch oft mit Datenschutz gleichgesetzt, bezeichnet aber den technischen Aspekt des Schutzes von Daten. Datensicherheit klärt beispielsweise die Frage, wie technisch sichergestellt werden kann, dass kein unberechtigter Zugriff auf Daten stattfindet. Im Gegensatz zum Datenschutz betrachtet Datensicherheit dabei auch Daten, die nicht personenbezogen sind.

b. Ziele von GUIDE

Die Erfassung des Menschen und seiner Handlungen ist für viele Forschungsfelder eine zwingende Voraussetzung. So werden beispielsweise im Smart-Home, in der Medizintechnik oder der interaktiven Robotik verschiedenste personenbezogene Daten verarbeitet. Gleichzeitig hat die Frage, wie Datenschutz in den Forschungsprojekten umzusetzen ist, mit der DSGVO an Bedeutung gewonnen.



Das Projekt GUIDE hat sich deshalb zum Ziel gesetzt, vor allem die Europäische Datenschutz-Grundverordnung zu analysieren und die wichtigsten Rechtsaspekte für Forschungsprojekte herauszuarbeiten. Der vorliegende Leitfaden fasst diese Ergebnisse zusammen, vermittelt zusätzliche Grundlagen und versucht Best Practices für wiederkehrende Aufgaben zu geben.

Natürlich kann dabei keine allumfassende Beratung zum Thema Datenschutz in Forschungsprojekten gegeben werden. Zum einen ist die DSGVO dafür zu umfassend und zum anderen sind je nach Forschungsgebiet neben der DSGVO noch bereichsbezogene Datenschutzregeln anzuwenden, wie beispielsweise Landesdatenschutz-

gesetze,Kirchendatenschutzgesetze und Datenschutzbestimmungen im Telemediengesetz, im Telekommunikationsgesetz und im Sozialgesetzbuch. Das Ziel von GUIDE ist es, eine erste Anlaufstelle für Wissenschaftler*innen zu sein, die zum ersten Mal mit dem Thema konfrontiert werden und für viele der Standardfragen eine Orientierung zu liefern.

c. Die Grundsatzfrage: Werden personenbezogene Daten verarbeitet?

Wie bereits erwähnt, regelt Datenschutz und damit auch insbesondere die DSGVO den Schutz natürlicher Personen und die Verarbeitung von personenbezogenen Daten. Art. 4 Nr. 1 DSGVO definiert den Begriff wie folgt:

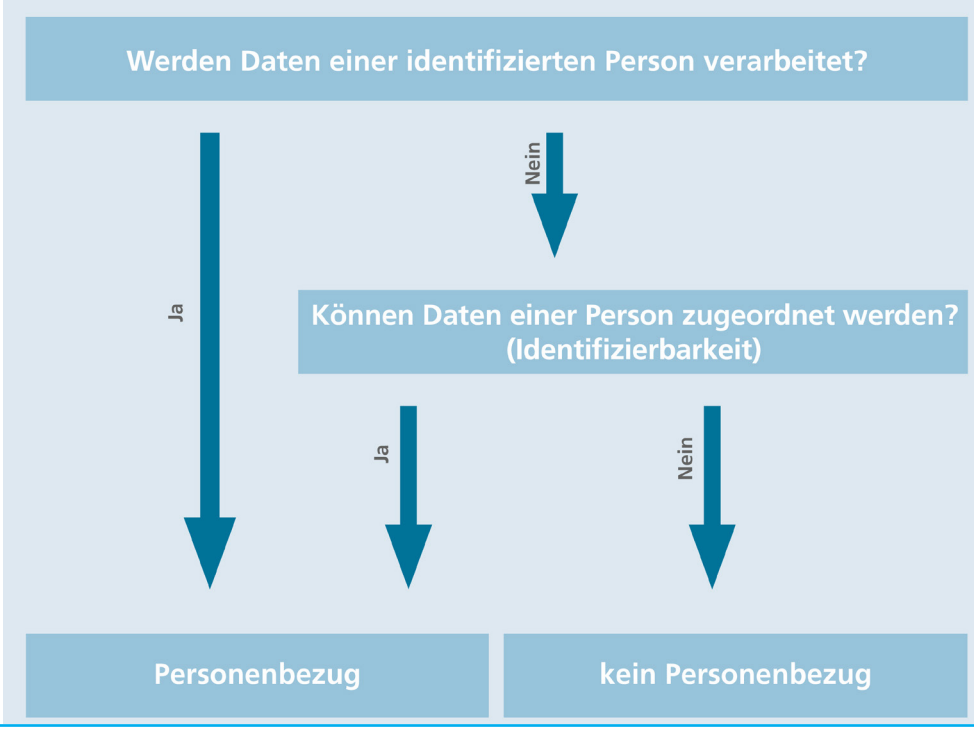
„personenbezogene Daten" [bezeichnen] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer 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."

Die Grenze zwischen personenbezogenen und nicht-personenbezogenen Daten ist dabei unscharf. Klar ist, dass beispielsweise ein Name oder eine Personalausweisnummer personenbezogen sind, weil sich diese Daten auf eine identifizierte natürliche Person beziehen.

Ebenfalls klar ist, dass beispielsweise eine Zugfahrkarte, die nur das Datum, Start- und Endbahnhof enthält, sich nicht auf eine identifizierte Person bezieht. Existiert jedoch in einem Unternehmen zu jeder Zugfahrkarte eine Reisekostenabrechnung, so kann möglicherweise über diese festgestellt werden, für wen die Karte gekauft wurde. Damit wird die Person hinter der Zugfahrkarte identifizierbar. Dabei spielt es keine Rolle, wer den Bezug zwischen Daten und Personen herstellen kann, ob man selbst oder nur Dritte dazu in der Lage sind, ist irrelevant. Eine Identifizierbarkeit ist nicht gegeben, wenn gesetzlich verbotene Mittel zur Identifizierung genutzt werden müssen oder die Identifizierung einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde. Dies entschied der Europäische Gerichtshof in einem Urteil 2016.[1]

Gerade bei Multimedia-Dateien ist die Frage, ob eine Identifizierbarkeit vorliegt, schwierig. Das Bild einer unbekannten Person ist beispielsweise dann ein personenbezogenes Datum, wenn Qualität und Auflösung vermuten lassen, dass Personen auf dem Bild von anderen erkannt werden können. Kann eine Identifizierung von Personen nicht sicher ausgeschlossen werden, sollte deshalb von einem Personenbezug ausgegangen werden.
Zusätzlich kennt die DSGVO noch besondere Kategorien personenbezogener Daten (Art. 9 DSGVO). Das sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Da bei solchen Daten besondere Risiken für die Rechte und Freiheiten natürlicher Personen gegeben sind, folgen spezielle Anforderungen an die Rechtmäßigkeit der Datenverarbeitung und an die Pflichten der Verantwortlichen.



[1]EuGH, Urteil vom 19.10.2016 - C-582/14 - Breyer

d. Bedeutung der DSGVO für die Forschung in der Mensch-Maschine-Interaktion

Bereits seit den 1970er Jahren ist Datenschutz ein aktives Forschungsfeld innerhalb einer klar abgetrennten Forschungsgemeinde. Diese Trennung wird vermutlich in den kommenden Jahren nachlassen. Zum einen ist es für Wissenschaftler*Innen wichtig zu verstehen, wann die eigene Forschungsarbeit unter der DSGVO privilegiert ist und wann für die Forschung Daten genutzt werden können, die beispielsweise in einem gewinnorientierten Industrieprojekt nicht genutzt werden dürfen.
Zum anderen stellt die Forschung einen idealen Zeitpunkt dar, um auch an den Datenschutz zu denken und ihn zu inkorporieren. Werden beispielsweise neue Verfahren entwickelt, um die körperliche Belastung eines Menschen zu messen, spielt es in der Forschungsphase aktuell nur eine untergeordnete Rolle, ob und welche personenbezogenen Daten verarbeitet werden. Kommt dieses Verfahren aber in die Anwendung, spielen Art und Umfang der Datenverarbeitung eine wichtige Rolle. Das macht Datenschutz zu einem interdisziplinären Thema mit hoher Relevanz für die Forschung.

2. Struktur und Nutzung

Kapitel 2 gibt einen Überblick zur Struktur der Leitlinien und wie diese von Wissenschaftler*innen genutzt werden können.

Diese im Rahmen des Projekts GUIDE erstellten Leitlinien sollen Wissenschaftler*Innen dabei helfen, die Aufgaben rund um den Datenschutz in der Forschung zu erfüllen. Die Leitlinien können dabei nicht alle datenschutzrechtlichen Fragen abschließend klären. Sie sollen als Nachschlagewerk und Sammlung von Best Practices für Wissenschaftler*innen in der Praxis dienen. Umfangreiche Themen sind jeweils als eigenständige, detaillierte Checklisten verfügbar. Sie finden diese in der Rubrik GUIDELines auf unserer Webseite:

www.guide-projekt.de.

Obwohl jedes Forschungsprojekt individuell ist, wurde an dieser Stelle der Versuch unternommen, die für den Datenschutz wichtigen Phasen eines Forschungsprojektes zu trennen. Kapitel 3 betrachtet zentrale Fragestellungen, die zum Projektstart geregelt werden müssen. Die wichtigste ist die Bestimmung des (datenschutzrechtlichen) Verantwortlichen. Dabei kommen zwei unterschiedliche Modelle in Betracht. Die Partner können jeweils eigenständig für die Verarbeitung verantwortlich sein oder das Konsortium verarbeitet personenbezogene Daten in sog. gemeinsamer Verantwortung. In Kapitel 3.a werden diese Optionen genauer betrachtet. Kapitel 3.b betrachtet die Rolle des Datenschutzbeauftragten.

Erst wenn die Grundlagen der Datenverarbeitung definiert sind, kann die Verarbeitung von personenbezogenen Daten begonnen werden. Dabei gehen die Leitlinien davon aus, dass jedes Forschungsprojekt mindestens eine sogenannte Verarbeitungstätigkeit hat. Eine Verarbeitungstätigkeit umfasst dabei jede Form der Datenverarbeitung, für die automatisiert oder teilautomatisiert personenbezogene Daten verarbeitet werden. Kapitel 4 betrachtet die Aufgaben, die im Zusammenhang mit solchen Verarbeitungstätigkeiten stehen. Kapitel 4.a betrachtet die Grundsätze der Datenverarbeitung, bevor Kapitel 4.b auf die Erstellung und Pflege des Eintrags in das Verzeichnis der Verarbeitungstätigkeiten eingeht. Kapitel 4.c beschreibt technische und organisatorische Maßnahmen für die IT-Sicherheit der personenbezogenen Daten. Kapitel 4.d untersucht die Anforderungen der DSGVO zur Sicherstellung der Rechte der Betroffenen und Kapitel 4.e zeigt die Anforderungen an die Einwilligung von betroffenen Personen in die Datenverarbeitung. Unter Umständen muss eine Datenschutz-Folgenabschätzung durchgeführt werden, dies wird in Kapitel 4.f betrachtet.
Am Ende einer Verarbeitungstätigkeit müssen bestimmte Aufräumarbeiten stattfinden. Kapitel 4.g betrachtet dazu die Löschung von personenbezogenen Daten und Kapitel 4.h geht auf die Anonymisierung ein. Kapitel 4.i beschreibt, wie unter besonderen Umständen personenbezogene Daten nach der Erreichung des Forschungsziels weiter genutzt werden dürfen.
Kapitel 5 betrachtet fortlaufende Hintergrundprozesse die unabhängig von den individuellen Verarbeitungstätigkeiten geregelt sein müssen.

3. Zentrale Aufgaben im Projekt

Dieses Kapitel betrachtet zentrale Aufgaben und Fragestellungen für Forschungsprojekte. Erst wenn diese grundlegenden Fragen geklärt sind, kann mit der Verarbeitung personenbezogener Daten begonnen werden.

a. Definition des für die Datenverarbeitung Verantwortlichen

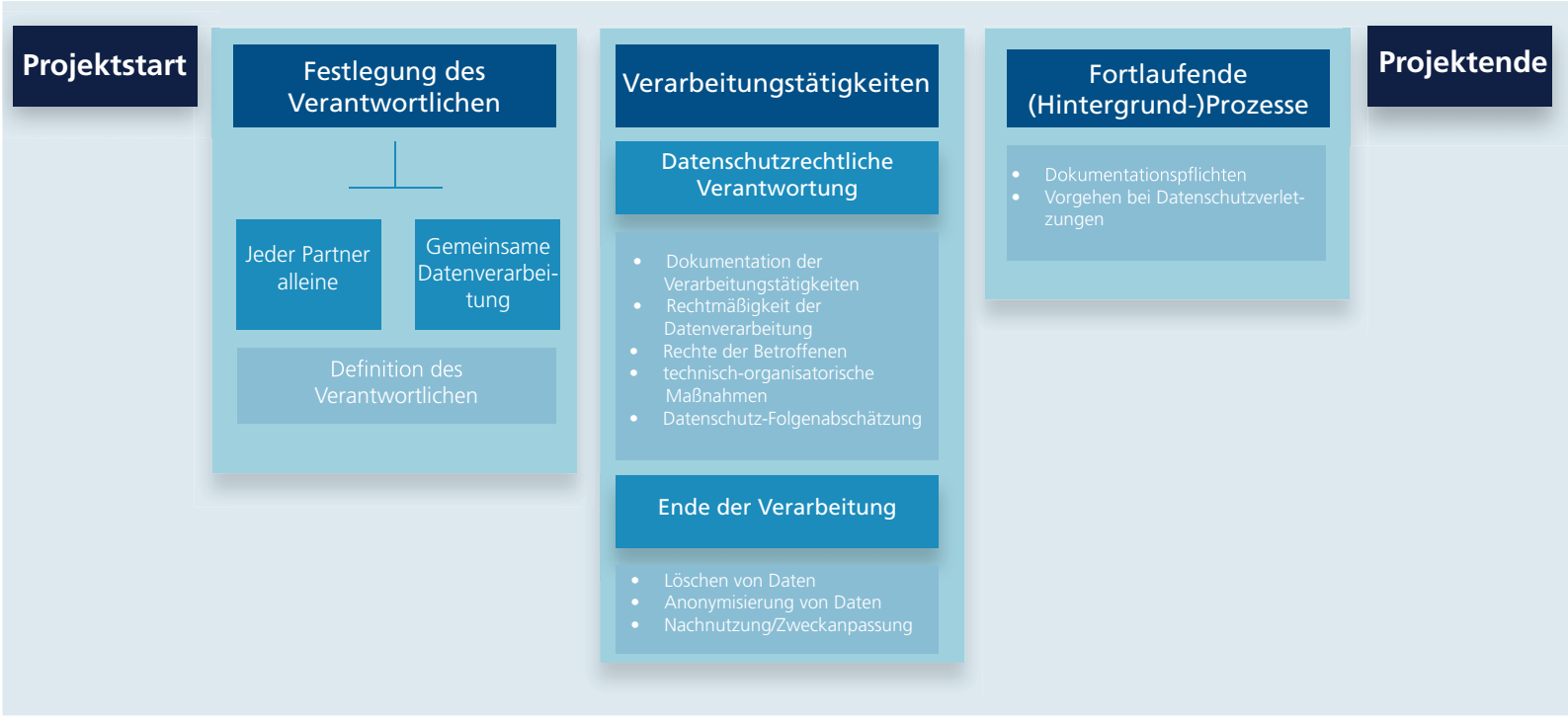
Der Verantwortliche beschreibt im Datenschutzrecht diejenige Person oder Institution, die personenbezogene Daten eigenständig verarbeitet. Als Verantwortlicher kann jede natürliche oder juristische Person, Behörde oder sonstige Stelle – unabhängig von ihrer Organisationsform – gelten (in der Forschung: Eine Hochschule, eine Stiftung, ein Verein, eine GmbH etc.). Entscheiden zwei oder mehr Verantwortliche gemeinsam über die Zwecke und Mittel der Verarbeitung, dann gelten sie als gemeinsam Verantwortliche.

Ausreichende Voraussetzung für die Qualifikation als Verantwortliche ist die tatsächliche Entscheidungsmacht über die Zwecke („Warum wird verarbeitet?“) und Mittel („Wie wird verarbeitet?“) der Verarbeitung personenbezogener Daten. Obliegt eine Verarbeitung damit im Wesentlichen dem Entscheidungsbereich einer Person oder Stelle, dann ist diese als Verantwortlicher zu qualifizieren. Nicht ausreichend für die Qualifikation als Verantwortlicher ist eine Verarbeitung auf Weisung einer anderen Person oder eine nur formale Entscheidungsmacht, die nicht ausgeübt wird.

i. Bestimmung des (datenschutzrechtlich) Verantwortlichen im Projekt

Inwiefern der Verantwortliche in einem Projekt bestimmt wird, ist davon abhängig, wie viele Forschungspartner am Projekt beteiligt sind und muss oftmals für den Einzelfall spezifisch entschieden werden. Ist nur eine Forschungseinrichtung an einem Projekt beteiligt, so gilt diese als eigenständig Verantwortliche im Projekt, wenn personenbezogene Daten verarbeitet werden.

Die geförderten Projekte der Mensch-Technik-Interaktion werden jedoch häufig als Verbundprojekt durchgeführt, an dem mindestens zwei Forschungseinrichtungen beteiligt sind, wovon eine das Projekt koordiniert (Verbundkoordinatorin). In solchen Konstellationen gilt zunächst: die Forschungseinrichtungen sind eigenständig Verantwortliche, wenn sie über Zwecke und Mittel der Datenverarbeitung allein entscheiden. Forschungseinrichtungen,



die keine personenbezogenen Daten verarbeiten, dürfen auch nicht Verantwortliche sein, da die DSGVO hier gar nicht anwendbar ist.
Je nach Struktur des Projekts kann regelmäßig aber eine gemeinsame datenschutzrechtliche Verantwortlichkeit der verarbeitenden Forschungspartner in einem Verbundprojekt begründet werden. Die Forschungspartner sind dann fortan nicht mehr eigenständig, sondern gemeinsam Verantwortliche im Sinne des Datenschutzrechts.

ii. Gemeinsame (datenschutzrechtliche) Verantwortlichkeit im Projekt

Ob die Forschungspartner als gemeinsam Verantwortliche zu betrachten sind, hängt davon ab, ob sie gemeinsam über Zwecke und Mittel der Verarbeitung entscheiden.
Der Zweck der Verarbeitung kann im Kooperationsvertrag festgelegt werden. Es kommt letztlich aber auf die tatsächlichen Umstände der Verarbeitung sowie die tatsächliche gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung an. Die europäische Rechtsprechung legt den Begriff der gemeinsam Verantwortlichen jedoch weit aus.[2] Zur Begründung einer gemeinsamen Verantwortlichkeit reicht es bereits aus, dass sich ein Forschungspartner an der Verarbeitung eines anderen Forschungspartners beteiligt und diese strukturell fördert bzw. ermöglicht. In vielen Verbundprojekten nutzen zwei oder mehr Verbundpartner dieselben personenbezogenen Daten. Es besteht daher Regelungsbedarf.

iii. Vereinbarung über die gemeinsame (datenschutzrechtliche) Verantwortlichkeit

Sofern die Forschungspartner in einem (Verbund-)Projekt als gemeinsame Verantwortliche gelten, müssen sie im Rahmen einer transparent gehaltenen Vereinbarung ihr innerorganisatorisches Verhältnis zueinander festlegen sowie Regelungen zur Erfüllung der datenschutzrechtlichen Pflichten treffen.
Die gemeinsame Verantwortlichkeit wird aber nicht erst durch die Vereinbarung begründet; sie entsteht bereits mit der tatsächlichen Entscheidung über die Zwecke und Mittel der Verarbeitung.
Zunächst muss insbesondere vereinbart werden, welcher Verantwortliche welche Informationspflichten (Art. 13 und 14 DSGVO) erfüllt und intern für die Wahrnehmung der Rechte der betroffenen Personen zuständig ist.
Obwohl hier zwar ein Ansprechpartner festgelegt wird, behält die betroffene Person die Befugnis, ihre Rechte bei und gegenüber jedem einzelnen Verantwortlichen geltend zu machen.
Wenn die Wahrnehmung der Rechte der betroffenen Personen und die Informationspflichten des Verantwortlichen geregelt sind, obliegt es den Forschungspartnern, wer welche weiteren datenschutzrechtlichen Pflichten wahrnimmt. Es kann also beispielsweise vereinbart werden, dass eine Arbeitsteilung erfolgt, oder dass jeder Forschungspartner für die Verarbeitungen in seinem Forschungsbereich oder Arbeitspaket eigenständig verantwortlich bleibt.

b. Die Rolle des Datenschutzbeauftragten in der Forschung

In Forschungsprojekten ist im Einzelfall zu prüfen, ob die Benennung eines Datenschutzbeauftragten nötig ist. Vorgaben zu der Benennung, den Aufgaben und der Stellung des Datenschutzbeauftragten sind in der DSGVO und im BDSG vorzufinden (zu den Aufgaben und der Stellung siehe **GUIDE-Checkliste „Datenschutzbeauftragter“**).
Das Gesetz bestimmt, unter welchen Voraussetzungen ein Datenschutzbeauftragter zu benennen ist. Art. 37 Abs. 1 DSGVO nennt hierfür folgende Szenarien:

- Die Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt (Buchstabe a)). **Hochschulen müssen daher zwingend einen Datenschutzbeauftragten benennen.** Dies gilt auch für ihre Beteiligung an einem Forschungsprojekt, in dem personenbezogene Daten verarbeitet werden.

- Die Kerntätigkeit des Verantwortlichen besteht in der Durchführung von Verarbeitungstätigkeiten, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Buchstabe b)). Dies gilt für privatrechtliche Stellen nur dann, wenn ihre „Kerntätigkeit“ entsprechend ausgerichtet ist.

- Die Kerntätigkeit des Verantwortlichen besteht in der Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Buchstabe c)). Dies gilt nur für Forschungsprojekte mit einer entsprechenden Zielsetzung, z.B. in der Medizin, in der Pflege oder in den Gesundheitswissenschaften.

Die Verarbeitung stellt dann eine Kerntätigkeit dar, wenn sie der Hauptzweck bzw. die Haupttätigkeit des Verantwortlichen ist. Nebensächliche, unterstützende und routinehafte Verarbeitungsvorgänge sind nicht als Kerntätigkeit zu verstehen.
Die DSGVO sieht in Art. 37 Abs. 4 eine Öffnungsklausel für das nationale Recht vor. Die Benennung des Datenschutzbeauftragten kann auf

[2] EuGH, Urteil vom 5.6.2018 - C-210/16 - ULD Schleswig Holstein/Wirtschaftsakademie Schleswig-Holstein

nationaler Ebene zusätzlich gesondert geregelt werden.
Insofern müssen nicht-öffentliche Stellen §38 BDSG zufolge eine/einen Datenschutzbeauftragten in weiteren Fällen zwingend benennen:

- Nicht-öffentliche Stellen benennen einen Datenschutzbeauftragten, soweit sie in der Regel mindestens **zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen** (§ 38 Abs. 1 S. 1 BDSG). Privatrechtlich organisierte Forschungsgruppen, in denen zahlreiche Forscher und Mitarbeiter regelmäßig personenbezogene Daten verarbeiten, dürften zur Benennung einer/-es Datenschutzbeauftragen zwingend verpflichtet sein.
- Eine Benennungspflicht liegt ebenfalls vor, wenn die verantwortliche nicht-öffentliche Stelle zur Vornahme einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO verpflichtet ist oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet (§ 38 Abs. 1 S. 2 BDSG).

Der benannte Datenschutzbeauftragte darf andere Aufgaben und Pflichten wahrnehmen, wenn diese nicht zu einem Interessenkonflikt führen. Der Datenschutzbeauftragte im Nebenamt ist damit rechtlich zulässig. Zulässig ist gleichfalls die Benennung eines einzigen, gemeinsamen Datenschutzbeauftragten für zusammengehörige Stellen. Es kann auch ein externer Datenschutzbeauftragter benannt werden.

c. Verschwiegenheitspflichten

Die an der wissenschaftlichen Forschung beteiligten Personen sind teilweise gesetzlich zur Verschwiegenheit verpflichtet. Dies gilt für Hochschulangehörige (Professoren, wissenschaftliche Mitarbeiter etc.) und bestimmte Berufsgruppen (Ärzte, Psychologen, Rechtsanwälte, Steuerberater etc.), aber nicht für andere mit der Projektarbeit befasste Personen (Doktoranden, studentische Hilfskräfte, Angestellte bei den privatrechtlich organisierten Verbundpartnern).
Es ist daher erforderlich, alle diejenigen, welche im Projektverlauf mit der Verarbeitung personenbezogener Daten befasst sind und keinen gesetzlichen Verschwiegenheitspflichten unterliegen, auf ihre diesbezüglichen Pflichten hinzuweisen und sie eine gesonderte Verschwiegenheitserklärung unterzeichnen zu lassen.

4. Individuelle Aufgaben für einzelne Verarbeitungstätigkeiten

Kapitel 4 untersucht die jeweils individuellen Aufgaben, die für die eigentliche Verarbeitung von personenbezogenen Daten in einer Verarbeitungstätigkeit wichtig sind.

Den datenschutzrechtlich Verantwortlichen treffen bei der Verarbeitung personenbezogener Daten verschiedene Pflichten nach der DSGVO. Auch hier gibt es die Rolle des Verantwortlichen, den laut DSGVO einige Pflichten treffen. Dieser Verantwortliche kann der bereits in Kapitel 3 für das Forschungsprojekt definierte sein. Es ist jedoch ebenfalls möglich, dass bei einer gemeinsamen Verantwortung innerhalb des Konsortiums (vgl. Kapitel 3.a.ii) für einzelne Verarbeitungstätigkeiten individuelle Verantwortungen definiert werden. Wichtig ist dabei nur, dass der Gesamtverantwortliche im Projekt über alle Verarbeitungstätigkeiten informiert ist und die Kommunikation sowie Zuständigkeiten untereinander abgestimmt ist.

a. Grundsätze für die Verarbeitung personenbezogener Daten

Das Datenschutzrecht geht davon aus, dass die Verarbeitung personenbezogener Daten immer mit einem Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht. Deshalb setzt es Anforderungen an die Verarbeitung personenbezogener Daten (Art. 5 DSGVO):
All diese Punkte sind durch den Verantwortlichen zu prüfen und zu dokumentieren (vgl. Kapitel 5.a).
Insbesondere beim Begriff der Rechtmäßigkeit gibt die DSGVO detailliertere Vorgaben. Es ist Aufgabe des Verantwortlichen, die Rechtmäßigkeit der Datenverarbeitung sicherzustellen. Unterschieden werden muss dabei zwischen Systemen die zusätzlich zu personenbezogenen Daten auch sensitive personenbezogene Daten verarbeiten.

- **Rechtmäßigkeit**
  Personenbezogene Daten dürfen nur verarbeitet werden, wenn ein entsprechender Erlaubnistatbestand vorliegt.
- **Verarbeitung nach Treu und Glauben**
  Dieser juristische Begriff ist für Laien schwer zu fassen und lässt sich nur im konkreten Einzelfall beurteilen. Es geht darum, ob ein bestimmtes Verhalten als anständig angesehen werden kann und ob nach bestem Wissen und Gewissen gehandelt wurde.
- **Transparenz**
  Der Grundsatz der Transparenz soll sicherstellen, dass betroffene Personen ihr Recht auf informationelle Selbstbestimmung wahrnehmen können und entsprechend über eine Datenverarbeitung informiert sind.
- **Zweckbindung**
  Der Zweck jeder Datenverarbeitung muss bereits beim Erheben der Daten definiert, eindeutig und legitim sein. Ausnahmen der Zweckbindung sind gerade in der wissenschaftlichen Forschung möglich. (vgl. Kapitel 4.i)
- **Datenminimierung**
  Die Datenverarbeitung muss dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
- **Richtigkeit**
  Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Unrichtige Daten müssen unverzüglich gelöscht werden.
- **Speicherbegrenzung**
  Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Auch bei diesem Grundsatz sind Ausnahmen für die wissenschaftliche Forschung möglich (vgl. Kapitel 4.i)
- **Integrität und Vertraulichkeit**
  Personenbezogene Daten sind so zu verarbeiten, dass eine angemessene Sicherheit gewährleistet ist. Dies umfasst auch den Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung der personenbezogenen Daten. (vgl. Kapitel 4.c)

i. Verarbeitung von personenbezogenen Daten (Art. 6 DSGVO)

Die einschlägigen Rechtsgrundlagen zur Legitimation der Verarbeitung personenbezogener Daten werden in Art. 6 DSGVO normiert. Für die Verarbeitung zu Forschungszwecken gilt zunächst nichts Anderes als wie für andere Zwecke, doch kommen meist folgende Erlaubnistatbestände infrage:

- **Einwilligung der betroffenen Person (Art. 9 Abs. 2 lit. a DSGVO)**
  Die Einwilligung dient der betroffenen Person als höchstpersönliches Mittel zur Legitimation der Verarbeitung sie betreffender personenbezogener Daten. Die betroffene Person kann somit jede Art der Datenverarbeitung grundsätzlich persönlich erlauben. Gerade wegen der weitreichenden Folgen, die eine Einwilligungserteilung haben kann, werden umfangreiche Anforderungen an ihre Form gerichtet. So wird sichergestellt, dass sich die betroffene Person auch der Tragweite

ihrer Entscheidung bewusst wird (siehe zu den Bedingungen die **GUIDE-Checkliste „Einwilligung“**). In der Summe muss die betroffene Person angeben, dass es sich um eine selbstbestimmte, freiwillige und ausdrückliche Erklärung handelt und sie mit der Verarbeitung der sie betreffenden Daten zu einem oder mehreren festgelegten Zwecken einverstanden ist.

- **Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DS-GVO) oder zur Wahrnehmung einer gesetzlich festgelegten Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 lit. e DSGVO)**

Eine Verarbeitung personenbezogener Daten kann auch zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse vorgenommen werden. Insbesondere öffentliche Forschungseinrichtungen (Hochschulen) haben einen gesetzlichen Auftrag zur Erfüllung ihrer Pflicht zur Forschung (vgl. Art. 6 Abs. 1 lit. c DSGVO i.V.m. §§ 3 Abs. 2, 70 Abs. 1 HG-NRW oder §§ 2 Abs. 1, 2 Abs. 5, 40 Abs. 1 HG-BW). Somit könnten Hochschulen aufgrund einer rechtlichen Verpflichtung zur Forschung personenbezogene Daten zu den von ihnen definierten Zwecken verarbeiten. Allerdings sind gegenüber der betroffenen Person die Informationspflichten gem. Art. 14 DSGVO einzuhalten.

- **Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des Verantwortlichen (Art. 6 Abs. 1 lit. f DSGVO)**

Daten dürfen verarbeitet werden, wenn die berechtigten Interessen des Verantwortlichen die Interessen der betroffenen Person an der Verarbeitung überwiegen (Interessenabwägung) und die geplante Verarbeitung muss vorgenommen werden, um den Zweck zu erreichen (Erforderlichkeit). Berechtigte Interessen können bspw. wirtschaftlicher oder ideeller Natur sein; sie müssen gewichtig genug sein um die Interessen der betroffenen Person zu überwiegen. Die Interessen der betroffenen Person äußern sich in der Wahrung ihrer Rechte und Freiheiten, vor allem in einer Respektierung ihrer Rechte auf informationelle Selbstbestimmung und Achtung der Menschenwürde.
Auf diesen Erlaubnistatbestand können sich maßgeblich privatwirtschaftlich organisierte Projektpartner berufen. Es ist auf Einzelfälle zu achten, in denen die Interessen der betroffenen Personen ggfs. höher gewichtet werden müssen (insb. Verarbeitung von sensitiven Daten oder Daten geschäftsunfähiger Personen). Die Interessenabwägung ist von dem Verantwortlichen zu dokumentieren. Zudem sind gegenüber der betroffenen Person die Informationspflichten gem. Art. 14 DSGVO einzuhalten.
Öffentliche Forschungseinrichtungen können sich von Gesetzes wegen nicht auf die Wahrung ihrer berechtigten Interessen berufen. Ihnen verbleibt jedoch die Möglichkeit, die Verarbeitung zur wissenschaftlichen Forschungszwecken auf Basis der bereits oben dargestellten Erlaubnistatbestände zu rechtfertigen.

ii. Verarbeitung sensitiver (personenbezogener) Daten (Art.9 DSGVO)

Bestimmte personenbezogene Daten, wie zum Beispiel medizinische Daten sind als sensitiver eingestuft als andere. Diese Daten dürfen nur nach folgenden Erlaubnistatbeständen verarbeitet werden:

- **Ausdrückliche Einwilligung der betroffenen Person (Art. 9 Abs. 2 lit. a DSGVO)**

Die Anforderungen an die Einwilligung bestimmen sich zunächst nach den allgemeinen Anforderungen des Art. 6 Abs. 1 lit. a i.V.m. Art. 7 und Art. 4 Nr. 11 DSGVO. Aufgrund der besonderen Natur der sensitiven Daten muss sich die Einwilligung jedoch gezielt auf deren Verarbeitung richten, sowie leicht erhöhten Maßstäben unterwerfen. Die Einwilligung muss ausdrücklich erteilt werden, und kann daher nicht konkludent erteilt werden. Aufgrund der Dokumentationspflicht empfiehlt sich die schriftliche Erteilung der Einwilligung. Zudem ist ein höheres Maß an Transparenz geboten, um der betroffenen Person die Tragweite ihrer Entscheidung bewusst zu machen. Schließlich verzichtet die betroffene Person auf einen besonderen Schutz, den ihre sensitiven Daten durch das Datenschutzrecht genießen.

- **Verarbeitung sensitiver Daten zu wissenschaftlichen Forschungszwecken (Art. 9 Abs. 2 lit. j DSGVO)**

Die DSGVO räumt dem nationalen Gesetzgeber die Möglichkeit ein, Rechtsgrundlagen zu schaffen, auf deren Basis sensitive Daten zu wissenschaftlichen Zwecken verarbeitet werden dürfen. Es handelt sich um eine explizite Privilegierung der Verarbeitung sensitiver Daten. Der deutsche Gesetzgeber hat von dieser Öffnungsklausel Gebrauch gemacht und die Verarbeitung sensitiver Daten zu wissenschaftlichen Zwecken erlaubt (§ 27 Abs. 1 BDSG, §17 Abs. 1 und 2 DSG-NRW, § 13 Abs. 1 LDSG-BW). Von diesem Forschungsprivileg sind insbesondere Projekte in den Bereichen Medizin, Pflege und Gesundheit erfasst, die für ihre Vorhaben überwiegend besondere Datenkategorien gem. Art. 9 DSGVO benötigen.
Die Verarbeitung muss regelmäßig angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten der Betroffenen unterliegen. Damit sind technische und organisatorische Maßnahmen gefordert, die grundsätzlich stärker ausgeprägt sein sollten als bei der Verarbeitung nicht-sensitiver Daten. Ferner wird

die Verarbeitung unter den Vorbehalt der Erforderlichkeit und einer positiven Interessenabwägung gestellt. Sensitive Daten dürfen zu wissenschaftlichen Zwecken verarbeitet werden, wenn die Verarbeitung dafür notwendig ist und die Interessen des Verantwortlichen die Interessen der Betroffenen (erheblich) überwiegen. Die jeweils einschlägigen Erlaubnistatbestände können sich in den verschiedenen Landesdatenschutzgesetzen in Detailfragen unterscheiden.

b. Erstellung und Pflege des Verzeichnisses der Verarbeitungstätigkeiten

Zu den regulären Pflichten des Verantwortlichen zählt nach Art. 30 DSGVO auch die Erstellung und Pflege eines Verzeichnisses aller Verarbeitungstätigkeiten.
Unter den Verarbeitungstätigkeiten im Sinne des Datenschutzes versteht man alle Vorgänge, in/bei denen personenbezogene Daten verarbeitet werden.

Verarbeitung ist gem. Art. 4 lit. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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.

Der Verantwortliche muss sich also fragen: Wo überall kommt das Forschungsprojekt mit Informationen über identifizierte oder identifizierbare natürliche Personen in Kontakt?
Das geschieht sowohl bei Experimenten, bei denen personenbezogene Daten verarbeitet werden, als auch während typischer „Verwaltungsprozesse". Wird beispielsweise ein Newsletter angeboten, zu dem sich Empfänger eintragen, stellt dieser Vorgang ein Verfahren dar. Das nachfolgende Muster für einen Eintrag im Verarbeitungsverzeichnis basiert auf einer Vorlage des Bayrischen Landesamts für Datenschutz und wurde im Kontext der Forschung kommentiert. Der Eintrag ist vor Start des Verarbeitungsverfahrens zu erstellen, also vor der Erhebung personenbezogener Daten und sollte regelmäßig sowie bei größeren Änderungen auf seine Aktualität hin überprüft werden.

c. Technische und organisatorische Maßnahmen (TOM) zur Datensicherheit

Die Forderung nach Maßnahmen zur Datensicherheit sind schon aus dem alten BDSG bekannt und werden in der DSGVO ähnlich behandelt. Gleich an mehreren Stellen, beispielsweise in Art. 24, Art. 25 und Art. 32 DSGVO findet man die Erwähnung von technischen und organisatorischen Maßnahmen (TOM). Diese fassen alle Maßnahmen zusammen, die der Verantwortliche umsetzen muss, um die Rechte und Freiheiten der betroffenen Personen zu schützen und sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt. Beispiele hierfür sind Maßnahmen und Nachweise zur Einhaltung der datenschutzrechtlichen Grundsätze gem. Art. 5 DSGVO, die Maßnahmen zur Einhaltung des Datenschutzrechts allgemein und deren Dokumentation (Art. 24 DSGVO), Maßnahmen der Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) und Maßnahmen der Datensicherheit (Art. 32 DSGVO), z.B. Verschlüsselung, Pseudonymisierung oder regelmäßige Backups der Daten.
Der Gesetzgeber fordert den Verarbeiter auf, selbst eine Interessensabwägung vorzunehmen und zu entscheiden, welches Schutzniveau angemessen ist. Hierbei sollte zuerst festgelegt werden, welche Daten für ein Forschungsprojekt zwingend erforderlich sind. Danach muss überlegt werden, welche Risiken durch die Verarbeitung der Daten für die Freiheiten und Rechte der betroffenen Personen entstehen und ob sich daraus physische, materielle oder immaterielle Schäden ergeben können. Der Gesetzgeber geht davon aus, dass durch jede Verarbeitung von personenbezogenen Daten mindestens ein geringes Risiko entsteht. Identifizierte Risiken können aber auch so gering sein, dass keine Maßnahmen erforderlich werden. Werden besonders sensitive Kategorien personenbezogener Daten verarbeitet (Art. 9 DSGVO) sollte immer von einem erhöhten Risiko ausgegangen werden.
Sind die Risiken identifiziert und bewertet, so müssen für jedes identifizierte Risiko geeignete Maßnahmen ausgewählt werden, um dieses zu verringern oder seine Eintrittswahrscheinlichkeit zu minimieren.
Die Auswahl der getroffenen Maßnahmen und ebenfalls verbleibende Restrisiken sind zu dokumentieren. Die Checkliste TOM zur Datensicherheit aus dem Anhang gibt Vorschläge zu möglichen Maßnahmen. Sie ist in ihrer Struktur an § 64 BDSG angelehnt.
Nach der Auswahl und Dokumentation der TOM sind diese dennoch weiterhin in regelmäßigen Intervallen und nach dem Bekanntwerden von Angriffen oder Sicherheitslücken zu überprüfen. So soll sichergestellt werden, dass das Schutzniveau der Daten nicht möglicherweise über die Zeit hinweg abgenommen hat oder dass bestimmte Maßnahmen weniger geeignet oder nutzlos geworden sind. In diesem Fall sollten zusätzliche TOM genutzt werden, um das Schutzniveau wieder auf das geforderte Maß zu bringen.

i. Datenverschlüsselung

Eine der Grundanforderungen der DSGVO ist, dass personenbezogene Dateien vor unbefugtem Zugriff durch Dritte geschützt gespeichert sind. Dies stellt innerhalb von Unternehmen und Forschungseinrichtungen meistens noch keine besondere Herausforderung dar. Typische etablierte TOM sind:

- Computer sind mit einer Passwortabfrage vor unberechtigtem Zugriff geschützt.
- Der Zugang (Zutritt) zu Rechenzentren wird nur absolut notwendigem Personal gewährt.
- Rechte und Rollen in IT-Systemen werden nach Anforderungen minimal vergeben.
- Regelmäßige Installation von sicherheitskritischen Updates.

Während die Verarbeitung von personenbezogenen Daten innerhalb von Organisationen meistens gut geschützt ist, bietet gerade die Weitergabe und die mobile Nutzung noch viele Fallstricke.
Computer und Laptops, die außerhalb einer Organisation genutzt werden, sollten komplett verschlüsselt werden. Das stellt sicher, dass die Festplatte nicht ausgebaut und an einem anderen PC genutzt wird. Mittlerweile bieten alle gängigen Betriebssysteme die Möglichkeit die gesamte Festplatte zu verschlüsseln. Bei hohen Anforderungen an die Sicherheit oder die Performance der Verschlüsselung können spezielle Festplatten, sogenannte Self Encrypting Devices, genutzt werden. Bei diesen wird die Verschlüsselung durch spezielle Chips auf der Festplatte übernommen, was eine hohe Geschwindigkeit und gute Sicherheit ermöglicht.
Eine weitere Herausforderung ist die verschlüsselte Übermittlung von personenbezogenen Dateien. Hier wird zuerst die Weitergabe von kleinen Dateien mittels Email betrachtet. Obwohl die Verschlüsselung von Emails eigentlich seit vielen Jahren technisch gelöst ist, ist dies selbst bei großen Firmen und Forschungseinrichtungen noch nicht durchgehend verfügbar. Eine Abhilfe ist, Dateien vor dem Versenden zu verschlüsselten und passwortgeschützten Archiven umzuwandeln. Das kann beispielsweise mit dem kostenlosen Open-Source Programm 7zip gemacht werden. Dabei ist natürlich darauf zu achten, ein ausreichend komplexes Passwort zu wählen und das Passwort dem Empfänger auf sichere Art und Weise zu übergeben.
Eine weitere Herausforderung ist der Einsatz mobiler Sensoren zur Datenaufzeichnung. Werden beispielsweise Videoaufnahmen gemacht, landen diese unverschlüsselt auf dem Speicher der Kamera. Hier ist darauf zu achten, dass keine unbefugten Personen Zugang zur Kamera haben und die Dateien so früh wie möglich auf eine geschützte Dateiablage übertragen werden. Der Kameraspeicher muss danach sicher gelöscht werden (vgl. Kapitel 4.e). Alternativ kann der Einsatz verschlüsselter Speicherkarten geprüft werden. Beispielsweise bietet der Hersteller swissbit microSD Speicherkarten an, die automatisch alle Dateien die darauf gespeichert werden verschlüsseln. Das Auslesen der Speicherkarte ist dann nur mit einer speziellen Software und einem vorher festgelegtem Passwort möglich.

d. Sicherstellen der Rechte der Betroffenen

Die Datenschutz-Grundverordnung räumt der betroffenen Person katalogartig umfassende Betroffenenrechte ein, die jederzeit zu erfüllen sind. Die auf Antrag einer betroffenen Person zu verwirklichenden Maßnahmen zur Erfüllung der Betroffenenrechte müssen von dem datenschutzrechtlich Verantwortlichen grundsätzlich unverzüglich ergriffen werden. Zugleich werden innerhalb der DSGVO aber Ausnahmen von den Betroffenenrechten ermöglicht, die es zu dokumentieren gilt.

i. Betroffenenrechte im Einzelnen

- **Auskunftsrecht des Betroffenen (Art. 15 DSGVO)**

Die betroffene Person kann vom Verantwortlichen eine umfassende Auskunft über die Verarbeitung seiner personenbezogenen Daten verlangen. Diese beinhaltet unter anderem: Die **Verarbeitungszwecke**; die **Kategorien** verarbeiteter personenbezogener Daten; die Empfänger oder Kategorien von Empfängern personenbezogener Daten; ggfs. die **Dauer der Speicherung** oder ggfs. die Kriterien für die Festlegung dieser Dauer.

- **Recht auf Berichtigung (Art. 16 DSGVO)**

Die betroffene Person kann die Berichtigung unrichtiger personenbezogener Daten verlangen. Der Verantwortliche muss diese unverzüglich berichtigen. Ferner kann die betroffene Person die Vervollständigung sie betreffender personenbezogener Daten verlangen.

- **Recht auf Löschung (Art. 17 DSGVO)**

Die betroffene Person kann grundsätzlich die Löschung sie betreffender personenbezogener Daten verlangen. Der Anspruch erstreckt sich zugleich auf öffentlich gemachte personenbezogene Daten sowie dazugehörige Links. Der Verantwortliche hat infolgedessen andere Verantwortliche über das Löschungsbegehren der betroffenen Person zu informieren.

- **Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)**

Die betroffene Person kann verlangen, dass die Verarbeitung sie betreffender personenbezogener Daten eingeschränkt bzw. gesperrt wird, wenn Daten **unrichtig** sind,

die Verarbeitung **unrechtmäßig** ist und der Betroffene aber die Löschung ablehnt, die Daten **nicht länger benötigt** werden und die betroffene Person die Daten aber zur Rechtsdurchsetzung benötigt **oder** ein **Widerspruch** gegen die Verarbeitung eingelegt wurde.

- **Recht auf Datenübertragbarkeit (Art. 20 DSGVO)**

Die betroffene Person kann verlangen, von ihr selbst bereitgestellte personenbezogene Daten in einem strukturierten und maschinenlesbaren Format zu erhalten, wenn die Verarbeitung auf Basis einer Einwilligung und automatisiert erfolgt. Ferner kann die betroffene Person verlangen, dass ihre personenbezogenen Daten ggfs. an andere Verantwortliche übersendet werden, soweit letzteres technisch realisierbar ist.

- **Widerspruchsrecht (Art. 21 DSGVO)**

Die betroffene Person kann Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einlegen. In diesem Fall kann der Verantwortliche die Verarbeitung nur durchführen, wenn er Gründe nachweist, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

ii. Ausnahmen für die wissenschaftliche Forschung

Für die wissenschaftliche Forschung eröffnet die DSGVO den Verantwortlichen Möglichkeiten, die Rechte der Betroffenen einzuschränken.
Sie räumt dem nationalen Gesetzgeber die Möglichkeit ein, bestimmte Betroffenenrechte entfallen zu lassen, wenn personenbezogene Daten zu wissenschaftlichen Zwecken verarbeitet werden und die Verarbeitung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen unterliegt (Art. 89 Abs. 2 i.V.m. Abs. 1 DSGVO). Zu den hiervon betroffenen Rechten gehören:

- Auskunftsrecht des Betroffenen
- Recht auf Berichtigung
- Recht auf Einschränkung der Verarbeitung
- Widerspruchsrecht

Der nationale Gesetzgeber hat von dieser Möglichkeit in § 27 Abs. 2 BDSG Gebrauch gemacht. In den für Hochschulen und öffentliche Stellen einschlägigen Landesdatenschutzgesetzen finden sich nahezu identische Vorschriften (vgl. § 13 Abs. 4 LDSG-BW). In Folge dessen sind Einschränkungen der Betroffenenrechte erlaubt, wenn die Verarbeitung personenbezogener Daten

- zu wissenschaftlichen Zwecken erfolgt und
- die Erfüllung der Betroffenenrechte die Erreichung des Forschungszwecks voraussichtlich unmöglich macht oder ernsthaft beeinträchtigt und
- die Beschränkung für die Erfüllung des Forschungszwecks notwendig ist und
- geeignete Garantien vorgesehen werden.

Unmöglichwerden oder Beeinträchtigung der Erreichung der Forschungszwecke: Ein Ausschluss der Betroffenenrechte ist nur erlaubt, wenn deren Verwirklichung sowie Erfüllung die Erreichung der wissenschaftlichen Zwecke unmöglich macht oder zumindest ernsthaft beeinträchtigt.
In dem Fall ist eine **zu dokumentierende** Prognose seitens der Forscher*innen vorzunehmen, ob

a) die Forschungszwecke ohne Beeinträchtigung der Betroffenenrechte verwirklicht werden können oder
b) Forschungszwecke nicht anders erfüllt werden können, weil sie eine Beschränkung der Betroffenenrecht notwendigerweise erfordern.

Notwendigkeit des Ausschlusses: Eine Ausnahme von der Gewährung der Betroffenenrechte ist nur legitim, wenn die Forschungszwecke nicht ohne die Beschränkung erreicht werden können (Verhältnismäßigkeitsgrundsatz).

Geeignete Garantien: Sollen die einzelnen Betroffenenrechte in der wissenschaftlichen Forschung entfallen, dann bedarf es zudem geeigneter Garantien zur Wahrung der (Grund-)Rechte und Freiheiten der betroffenen Personen.

Zu den geeigneten Garantien im Sinne des Gesetzes gehören technische und organisatorische Maßnahmen (TOM), die insbesondere den Grundsatz der Datenminimierung gewährleisten, z.B. die Pseudonymisierung.
Das Recht auf Auskunft kann zudem entfallen, wenn die Daten für die Erreichung des wissenschaftlichen Forschungszwecks erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. (Dies ist bspw. nicht in § 17 Abs. 5 DSG NRW umgesetzt, aber in § 13 Abs. 4 LDSG-BW.)
Der Anspruch der betroffenen Person auf Löschung gem. Art. 17 Abs. 1 DSGVO kann auf Grundlage einer gesonderten Regelung entfallen. Er besteht nicht, wenn die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken erfolgt und die Löschung die Verwirklichung des Forschungszwecks voraussichtlich unmöglich macht oder ernsthaft beeinträchtigt (Art. 17 Abs. 3 lit. d i.V.m. Art. 89 Abs. 1 DSGVO).

iii. Organisatorische Umsetzung

In Projekten der wissenschaftlichen Forschung muss die Ausnahme von der Gewährung der Betroffenenrechte begründet und dokumentiert werden; außerdem muss sichergestellt sein, dass es geeignete Garantien für die Rechte und Freiheiten natürlicher Personen gibt (vgl. oben).
Unabhängig hiervon hat der datenschutzrechtlich Verantwortliche sicherzustellen, dass die Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten auch in der Forschung gewahrt werden.
Werden die Betroffenenrechte gewährt, sind diese auch in der Forschung unverzüglich zu verwirklichen. Der Verantwortliche hat generell Sorge dafür zu tragen, dass alle mit den Betroffenenrechten verbundenen Informationen und Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen (Art. 12 Abs. 1 DSGVO). Grundsätzlich muss der Verantwortliche den betroffenen Personen auch die Ausübung ihrer Rechte weitestgehend erleichtern (Art. 12 Abs. 2 DSGVO) sowie Anträge unverzüglich, jedenfalls spätestens einen Monat nach Eingang des Antrags, beantworten.
Hieraus folgen zentrale Vorgaben für die Sicherstellung der Betroffenenrechte:

- **Zuweisung von Zuständigkeiten:**
Der Verantwortliche muss organisatorisch Sorge dafür tragen, dass Betroffenenrechte bearbeitet werden können. Daher empfiehlt es sich, klare Zuständigkeiten zu schaffen, wer für diese Aufgabe innerorganisatorisch verantwortlich ist. Oftmals kann dies über eine zentrale Ansprechperson realisiert werden, die ohnehin für die datenschutzrechtlich relevanten Vorgänge im Projekt verantwortlich ist. Diese Person sollte ohnehin bereits einen umfassenden Überblick über die Strukturen und Prozesse haben. In den Best Practices im Anhang werden diese Aufgaben an den sogenannten Datenmanager delegiert.

- **Kommunikationskanäle:**
Aus dem Gebot, der betroffenen Person die Ausübung der Rechte zu erleichtern folgt, dass ein entsprechender transparenter Kommunikationskanal zur betroffenen Person geschaffen werden muss. Der betroffenen Person muss ersichtlich sein, an wen sie sich wenden und unter welchen Möglichkeiten (z.B. telefonisch, per E-Mail, Kontaktformular) dies geschehen kann. Der Aufwand für die betroffene Person sollte weitestgehend reduziert werden.

- **Bearbeitungsfristen:**
Die Anträge der betroffenen Person zur Erfüllung ihrer Betroffenenrechte sollen in der Regel unverzüglich, in einzelnen Fällen aber spätestens einen Monat nach Antragseingang beantwortet werden. Notwendig sind damit organisatorische Vorgaben zur tatsächlichen unverzüglichen Bearbeitung und Benachrichtigung der betroffenen Person über ergriffene Maßnahmen, um Rechtsverstöße zu vermeiden. Da Benachrichtigungen regelmäßig unverzüglich zu erfolgen haben, folgt hieraus auch, dass die vorgelagerte Bearbeitung sowie die Ergreifung entsprechender Maßnahmen unverzüglich nach Antragseingang vorgenommen werden muss.

Sonderfälle zur Sicherstellung der Betroffenenrechte können sich im Rahmen der gemeinsamen Verantwortung ergeben. Wie in Kapitel 3.a.iii bereits aufgezeigt, müssen die Verbundsmitglieder eine Vereinbarung über die internen Zuständigkeiten für Wahrnehmung und Erfüllung der Betroffenenrechte formulieren und gegebenfalls eine Anlaufstelle für betroffene Personen angeben.
Der betroffenen Person wird von Gesetzes wegen dennoch die Möglichkeit eingeräumt, ihre Rechte bei und gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen. Damit müssen im Ergebnis innerhalb eines Verbundprojekts Kommunikationswege geschaffen werden, um die Anfragen der betroffenen Personen an den zuständigen Projektpartner weiterzuleiten.

e. Datenschutz-Folgenabschätzung

Eine weitere Neuerung der DSGVO gegenüber dem früheren Datenschutzrecht sind die Datenschutz-Folgenabschätzungen (DSFA), wie sie in Art. 35 DSGVO geregelt sind. Eine Datenschutz-Folgenabschätzung ist ein formales Vorgehen, um die Risiken für Rechte und Freiheiten betroffener Personen zu sammeln und zu bewerten. Damit soll vor der Inbetriebnahme einer Verarbeitungstätigkeit sichergestellt werden, dass keine für die betroffenen Personen untragbaren Risiken existieren.

Das Gesetz selbst fordert diese für Systeme, die durch die Art und den Umfang der angedachten Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen haben. Eine DSFA wird beispielsweise bei umfangreicher systematischer Überwachung öffentlicher Bereiche gefordert, wenn Systeme extensive Verarbeitung sensitiver Kategorien von personenbezogenen Daten (Art. 9 DSGVO) vornehmen oder wenn Systeme (auf Grundlage einer Bewertung der persönlichen Umstände natürlicher Personen) automatische Entscheidungen treffen, die aber Rechtswirkung gegenüber diesen entfalten.
Laut Gesetz muss von der zuständigen Aufsichtsbehörde auch eine Liste mit Technologien veröffentlicht werden, bei deren Benutzung eine DSFA verpflichtend ist. Diese sog. DSFA-Positivliste ist für

den öffentlichen Bereich beispielsweise auf der Webseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zu finden.[3]
Die Bedeutung der DSFA für die Forschung ist zum aktuellen Zeitpunkt noch nicht klar. Es ist zu vermuten, dass DSFAs für die Grundlagenforschung im Mensch-Technik-Kontext nicht relevant sind. Gerade Experimente mit freiwilligen Probanden bergen vermutlich kein derart hohes Risiko, dass der Aufwand gerechtfertigt wäre.
Im Bereich der Pflege jedoch ist die Frage der Notwendigkeit einer DSFA schwer zu beantworten. Hier werden oftmals Systeme entwickelt und getestet, die fortlaufend Menschen beobachten und aus ihrem Verhalten lernen. Hier bleibt eine Entscheidung der Aufsichtsbehörden abzuwarten. Eindeutiger ist die Situation in der Medizinforschung. Gerade dann, wenn umfassende Probendatenbanken von Patienten erstellt werden sollen, ist eine DSFA unerlässlich.

f. Veröffentlichungen

Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.
Der Regelfall ist also eine – spezielle – Einwilligung der betroffenen Personen in die Nutzung ihrer personenbezogenen Daten für die vorgesehene Veröffentlichung.

g. Löschen von personenbezogenen Daten

Bei jeder Verarbeitung personenbezogener Daten kommt der Zeitpunkt, ab dem die Daten nicht länger gespeichert werden dürfen. Das kann je nach Projekt und Erlaubnistatbestand ganz unterschiedliche Gründe haben:

- Die Daten werden für den Zweck, für den sie erhoben wurden, nicht mehr benötigt,
- die in der Einwilligung angegebene Speicherdauer ist erreicht,
- eine Einwilligung in die Datenverarbeitung wurde widerrufen,
- die betroffene Person begehrt die Löschung ihrer personenbezogenen Daten.

Ist einer oder mehrere dieser Fälle eingetreten, müssen alle personenbezogenen Daten entweder gelöscht oder vollständig anonymisiert werden. Dabei sind einige Punkte zu beachten.

- Es kann möglich sein, dass Daten aus gesetzlichen Gründen länger aufbewahrt werden müssen, als dies für die Forschungsaufgabe notwendig ist. In diesem Fall ist sicherzustellen, dass die Daten nicht mehr für den Zweck der Forschung verwendet werden, aber die gesetzlichen Aufbewahrungsfristen erfüllt sind. Probanden sollten auch über eine solche Archivierung informiert werden.
- Werden Daten von mehreren Forschungseinrichtungen genutzt und möglicherweise sogar bei mehreren Verbundpartnern verteilt verarbeitet, muss sichergestellt werden, dass alle Kopien der Daten entsprechend vernichtet werden.
- Daten müssen nicht nur aufbewahrt werden, um der Auskunftspflicht nachzukommen. Die Löschung nicht mehr benötigter, personenbezogener Daten ist wichtiger als die Erteilung von Auskünften an die betroffenen Personen. Sollte nach der Löschung ein Auskunftsanspruch geltend gemacht werden, reicht es, den Anfragenden über die Löschung der Daten zu informieren.

Im einfachsten Fall ist das Ziel der wissenschaftlichen Forschung erreicht und es liegen keine Aufbewahrungsfristen vor. In diesem Fall müssen die erfassten Daten gelöscht werden. Das Gesetz gibt dabei keine genauen Vorgaben, wie sicher gelöscht wird. Hierbei sollte beachtet werden, dass eine Löschung oder Formatierung mit verbreiteten Betriebssystemen alleine, noch keine sichere Löschung garantiert. Bei diesen Verfahren können teilweise Daten wiederhergestellt werden. Das BSI gibt Tipps zur sicheren Löschung von Daten und Datenträgern:

http://s.fhg.de/richtigloeschen [4]

h. Anonymisierung von Daten

Eine Alternative zur Löschung stellt die Anonymisierung dar. Dabei müssen die Daten so verändert werden, dass zu den individuellen Personen keinerlei Bezug mehr hergestellt werden kann. Die Anforderungen des Gesetzes an die Anonymisierung sind dabei sehr hoch.
So lange die betroffene Person vernünftigerweise identifiziert werden kann, sind dessen Daten nicht anonymisiert. Das ist immer dann der Fall, wenn eine Re-Anonymisierung mit einem verhältnismäßigen Aufwand (Zeit, Kosten, verfügbare Technologie) vorgenommen werden kann. Komplette Anonymisierung ist nur dann gegeben, wenn eine Re-Anonymisierung nur unter unverhältnismäßigem Aufwand oder mit der Verwendung illegaler Mittel vorgenommen werden kann. Dies bedeutet besonders für Audio- und Videoaufnahmen von Menschen, dass nahezu keine zuverlässige Anonymisierung erreicht werden kann, ohne die Daten für eine (wissenschaftliche) Auswertung nutzlos zu machen. So können beispielsweise selbst bei extrem schlechter Auflösung, Personen in

[3] http://s.fhg.de/nrw-dsfa

Videos an ihrem Gang oder charakteristischer Kleidung erkannt und identifiziert werden. Sobald Personen aber identifizierbar sind, liegen personenbezogene Daten vor und es ist ein Erlaubnistatbestand für ihre Verarbeitung notwendig. Sind Daten aber erfolgreich anonymisiert, entfallen die Vorgaben der DSGVO und sie dürfen unbegrenzt genutzt und geteilt werden.

i. Nachnutzung/ Zweckanpassung

Personenbezogene Daten dürfen grundsätzlich nur für die Zwecke verarbeitet werden, für die sie erhoben worden sind (Grundsatz der Zweckbindung) sowie auch nur so lange gespeichert werden, bis der Zweck erreicht ist, also spätestens zum Projektabschluss (Grundsatz der Speicherbegrenzung). Eine Weiterverarbeitung dieser Daten zu einem anderen Zweck ist daher nur möglich, wenn dieser mit dem Erhebungszweck aufgrund einer sachlichen Verbindung zwischen beiden Zwecken vereinbar ist (Kompatibilität). Zudem sind die Interessen der betroffenen Person bei der Bewertung der Kompatibilität zu berücksichtigen. Gerade in Forschungsprojekten können oftmals personenbezogene Daten verarbeitet werden, die bereits zu anderen Zwecken erhoben worden sind. Für den Bereich der Forschung wird aber eine Privilegierung normiert, sodass die zu einem bestimmten Zweck erhobenen Daten zu wissenschaftlichen Forschungszwecken weiter genutzt werden dürfen und nicht gelöscht werden müssen.

i. Forschungsprivileg

Sofern die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken stattfindet, wird sie explizit gesetzlich privilegiert. Innerhalb dieses sog. Forschungsprivilegs sind unter anderem zwei Erleichterungen von Bedeutung:

- Art. 5 Abs. 1 lit. b DSGVO normiert zunächst eine weitgehende Aufhebung der Zweckbindung für Daten, die ursprünglich für andere Zwecke verarbeitet wurden. Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke sowie für Zwecke der Statistik ist erlaubt. (sog. „Nachnutzung").
- Art. 5 Abs. 1 lit. e DSGVO normiert einhergehend mit der Nachnutzung das Entfallen der Speicherbegrenzung. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie ausschließlich für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden.

ii. Begriff der wissenschaftlichen Forschung

Das Forschungsprivileg gilt immer dann, wenn personenbezogene Daten zu wissenschaftlichen Forschungszwecken verarbeitet werden. Die „wissenschaftlichen Forschungszwecke" sind weit gefasst zu verstehen. Hierunter sind – unter anderem und auch nicht abschließend – die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung eingeschlossen.
Der europäische Begriff der Forschung beschränkt sich nicht auf bestimmte akademische Einrichtungen, Auftraggeber, Forschungsziele oder Rechtsformen. Hier kommt es darauf an, ob die Forschung das Ziel hat, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen. Es muss nach Inhalt und Form ein ernsthafter Versuch zur Ermittlung von Wahrheit unternommen werden.
Es ist daher darauf zu achten, dass Forschungseinrichtungen ernsthaft um eine wissenschaftlich fundierte Forschung und methodische Suche nach Erkenntnissen und der Wahrheit bemüht sind und nicht allein aufgrund wirtschaftlicher Faktoren Forschung betreiben.

iii. Weitere Voraussetzungen

Wenn das Forschungsprivileg für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken genutzt werden soll, müssen die Verantwortlichen durch sogenannte geeignete Garantien den Schutz der Betroffenenrechte sicherstellen. Dabei handelt es sich vornehmlich um organisatorische sowie technische Maßnahmen (TOM) zur Einhaltung der datenschutzrechtlichen Anforderungen bei der Verarbeitung. Bei der Verarbeitung in der Forschung müssen diese TOM jedoch spezifischer und verschärfter ausfallen, als TOM, die zur Verarbeitung „gewöhnlicher" personenbezogener Daten getroffen werden. Dies stellt gewissermaßen einen Ausgleich zu
Die Nachnutzung personenbezogener Daten zu wissenschaftlichen Forschungszwecken wird darüber hinaus unter einen Vorbehalt gestellt. Der Verantwortliche hat zunächst zu prüfen, ob die wissenschaftlichen Zwecke mit anonymen oder anonymisierten Daten erreicht werden können. Ist dies nicht der Fall, können personenbezogene Daten „nachgenutzt" werden.

5. Fortlaufende (Hintergrund-) Prozesse

In Forschungsprojekten erfolgt eine fortlaufende Dokumentation der Aufgaben und der erzielten Ergebnisse. Kapitel 5 gibt eine Übersicht über die notwendigen Schritte.

a. Dokumentationspflichten

Der Verantwortliche hat sicherzustellen, dass die Datenverarbeitungsprozesse den Vorgaben der Datenschutz-Grundverordnung (DSGVO) entsprechen, Art. 24 Abs. 1 DSGVO. Die geeigneten technischen und organisatorischen Maßnahmen sind zu dokumentieren:

- Verzeichnis der Verarbeitungstätigkeiten, Art. 30 DSGVO,
- Rechtmäßigkeit der Verarbeitung, z.B. durch Dokumentation der Einwilligung oder eines anderen Erlaubnisvorbehaltes (Art. 5 lit. a DSGVO),
- Transparenz durch Erfüllung der Informationspflichten (Art. 5 lit. a DSGVO),
- Maßnahmen zur Sicherstellung der Richtigkeit der personenbezogenen Daten und zur Berichtigung oder Löschung, falls die Daten unrichtig sind (Art. 5 lit. d DSGVO),
- Maßnahmen zur Speicherbegrenzung oder zur Ausnahme nach dem Forschungsprivileg (Art 5 lit. e DSGVO),
- Ausnahmen von den Betroffenenrechten nach dem Forschungsprivileg (Art. 89 Abs. 2 DSGVO),
- Maßnahmen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO),
- ggf. Datenschutz-Folgenabschätzung (Art. 35 ff DSGVO),
- Integrität und Vertraulichkeit (Art. 5 lit. f DSGVO), Sicherheit der Verarbeitung (Art. 32 ff DSGVO) und ggf. Sicherheitsverletzungen.

b. Vorgehen bei Datenschutzverletzungen

Eine Datenschutzverletzung schließt jede Verletzung der Sicherheit ein, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führt.
Werden Datenschutzverletzungen bekannt, sind mehrere Schritte zu unternehmen. Die Verletzung muss dokumentiert werden, unabhängig von ihrer Schwere.
Weiter muss überlegt werden, ob neue oder geänderte TOM benötigt werden, um zukünftig das Auftreten dieser oder ähnlicher Datenschutzverletzungen zu vermeiden. In besonderen Fällen ist auch eine Meldung an die Aufsichtsbehörde und die betroffenen Personen erforderlich.

i. Meldung an die Aufsichtsbehörde

Der Verantwortliche muss eine Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde melden, nachdem ihm die Verletzung bekannt wurde (Art. 33 DSGVO).
Eine Verletzung des Schutzes personenbezogener Daten liegt dann vor, wenn gegen die Grundsätze der Datensicherheit verstoßen wird und diese Verletzung zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang von bzw. zu personenbezogenen Daten führt (im Folgenden: Datenpanne). Ein Verschulden des Verantwortlichen ist für die Pflicht zur Meldung nicht ausschlaggebend. Auch eine versehentliche Datenpanne muss gemeldet werden.
Die Datenpanne wird dem Verantwortlichen bekannt, wenn hinreichende Kenntnis von den tatsächlichen Umständen der Panne erlangt worden ist. Reine Verdachtsmomente begründen damit noch keine Pflicht zur Meldung. Eine Meldung muss ebenfalls nicht abgegeben werden, wenn eine Datenpanne nach einer eigenverantwortlichen Prognose des Verantwortlichen nur zu einem geringen Risiko für die betroffenen Personen führt. Ein Risiko in diesem Sinne äußert sich dadurch, dass die Grundrechte verletzt werden (insbesondere das Recht auf informationelle Selbstbestimmung).

Die Meldung hat unverzüglich und spätestens **innerhalb von 72 Stunden** nach Bekanntwerden des Verstoßes zu erfolgen; eine Verzögerung muss unter Darstellung besonderer Umstände begründet werden. Inhaltlich sind der Meldung umfangreiche Informationen und Beschreibungen beizufügen, die unter anderem die **Art der Verletzung** sowie die **Anzahl der von der Verletzung betroffenen Personen**, die wahrscheinlichen Folgen der Verletzung sowie die **ergriffenen Maßnahmen zur Behebung** der Verletzung darstellen.

ii. Meldung an die betroffene Person

Eine weitere, separate Meldung muss an die betroffenen Personen übermittelt werden, wenn die Datenpanne ein hohes Risiko für die Grundrechte der betroffenen Personen impliziert (Art. 34 DSGVO). Auch hier muss der Verantwortliche eine eigenverantwortliche Prognose zur Beurteilung des Risikos der Datenpanne vornehmen. Anders als in Art. 33 muss das Risiko aber voraussichtlich als hoch bewertet werden, um eine Meldungspflicht auszulösen.

Das Gesetz selbst erlässt dem Verantwortlichen eine Meldung an die einzelnen betroffenen Personen, wenn im Anschluss an das Bekanntwerden der Datenpanne wirksame technische und organisatorische Maßnahmen (TOM) ergriffen wurden, um die Missstände sowie das hohe Risiko für die betroffenen Personen zu beseitigen. Ist der Aufwand, die Datenpanne bei den betroffenen Personen zu melden unverhältnismäßig hoch, so können andere öffentlich zugängliche oder wahrnehmbare Formen der Kommunikation genutzt werden. Voraussetzung ist hier, dass sie einen vergleichbar wirksamen Effekt erzielen wie eine spezifische Meldung.

Der Inhalt der Meldung gestaltet sich vergleichbar zur Meldung an die Aufsichtsbehörde, jedoch muss eine klare, verständliche und einfache Sprache genutzt werden, um den betroffenen Personen die Informationen zur Datenpanne nachvollziehbar und begreiflich vermitteln.

6. Anhang

Der Anhang der Leitlinien fasst Best Practices sowie einige Musterklauseln zusammen. Er dient dazu, Wissenschaftler*innen konkrete Beispiele über die Ausgestaltung der wichtigsten Dokumente zu geben.

Kapitel 6.a beschreibt dazu eine Möglichkeit, wie in einem Forschungsprojekt mit gemeinsamer Verantwortung die Nutzung der Daten organisiert ist. Kapitel 6.b zeigt ein Beispiel einer Informations- und Einwilligungsschrift für die Teilnehmer*Innen in einem Experiment. Kapitel 6.c und 6.d geben Beispiele für die vertragliche Regelung der Datennutzung. Der Datennutzungsvertrag in Kapitel 6.c geht dabei davon aus, dass die gemeinsame Datennutzung nicht zentral geregelt ist. Kapitel 6.d zeigt, wie die Datennutzung in einem zentralen Dokument, beispielsweise dem Konsortialvertrag geregelt werden kann.
Kapitel 6.e ist ein kommentiertes Muster für den Eintrag in das Verzeichnis der Verarbeitungstätigkeiten. Kapitel 6.f ist eine Checkliste zur Dokumentation der TOM zur Datensicherheit gemäß Art. 32 DSGVO. Diese gibt eine Auswahl möglicher Maßnahmen, um die geforderten Sicherheitsziele zu erreichen. Es müssen dabei nicht alle gelisteten Maßnahmen erfüllt werden, sondern der Verantwortliche wählt die für seine Verarbeitungstätigkeit passenden aus und erweitert die Liste gegebenfalls um zusätzliche. Beispielsweise wird nicht immer eine Alarmanlage vorhanden sein, um die Zugangskontrolle zur Verarbeitungsanlagen durchzusetzen. Eine mögliche Alternative wäre, dass alle Serverschränke verschlossen sind und nur befugte Personen einen Schlüssel haben.

6.a Best Practices Datenmanager

Eine typische Herausforderung für öffentliche Forschungsprojekte ist die verteilte Verarbeitung personenbezogener Daten durch mehrere Partner im Projekt. Im Folgenden wird das fiktives Forschungsprojekt „Persönliche Assistenz (PASS)“ beschrieben und wie dieses die gestellten Anforderungen durch den Einsatz eines Datenmanagers erfüllt. Dieser agiert als zentraler Ansprechpartner nach Innen und nach Außen für alle Belange der Datenverarbeitung.
In PASS wollen Forscher der FH Bielefeld und des Fraunhofer IOSB gemeinsam Assistenzsysteme in einer intelligenten Küche untersuchen. Dabei soll untersucht werden, ob man aus den Essensgewohnheiten der Bewohner und daraus, welche Lebensmittel aus dem Kühlschrankes entnommen werden, darauf schließen kann, welches Gericht der Bewohner als nächstes kocht. Im ersten Experiment „Smarte Küche“, werden erste Daten mit Freiwilligen erhoben, um das System zu entwickeln. Forscher beider Einrichtungen sind an der Erhebung und der geplanten Datenauswertung beteiligt. Nach außen wird das Fraunhofer IOSB als Ansprechpartner und Verantwortlicher für die Datenverarbeitung genannt.
Im Experiment werden nacheinander die Daten von mehreren Freiwilligen erhoben. Vor dem Start der Datenerhebung erhält jeder Freiwilliger zuerst eine Informationsschrift über das Experiment und wird gebeten, eine Einwilligung zu unterschreiben. (vgl. Kombiniertes Informations- und Einwilligungsdokument.) Diese informiert über das Experiment, die erfassten Daten, Speicherdauern und auch darüber, mit wem die Daten geteilt werden. Nur wenn die Einwilligung ausgefüllt wird, darf ein Freiwilliger an der Datenerhebung teilnehmen. Zusätzlich wird ein zufälliges Pseudonym erzeugt, um die erfassten Daten dem Probanden zuordnen zu können. Dieses wird später für die Aufgaben des Datenmanagers wichtig sein.
Zum Start der Datenerhebung werden mit einem Fragebogen zuerst die Essengewohnheiten der Probanden erhoben. Auf diesem Fragebogen werden keine Namen. notiert, sondern nur das Pseudonym des Probanden. Nach dem Ausfüllen des Fragebogens treffen die Probanden in der Küche alle Vorbereitungen, um ein von ihnen gewähltes Gericht zu kochen. Sie werden dabei durch verschiedene Sensoren beobachtet und die Daten werden für die spätere Auswertung aufgezeichnet. Die Sensordaten jedes Probanden werden so gespeichert, dass sie seinem individuellen Pseudonym zugeordnet sind. Am Ende der Datenerhebung werden alle erfassten Sensordaten, einschließlich der Fragebögen und der Einwilligungen an den Datenmanager übergeben. Dieser ist somit initial die einzige Stelle, bei der Daten gespeichert sind und kontrolliert die Weitergabe an die Partner. Die unterschriebene Einwilligung der Probanden ist die einzige Stelle, an der Namen und gegebenenfalls

Adressen der Probanden geführt werden. Sie verbleibt ausschließlich beim Datenmanager. Die Forscher erhalten für ihre weitere Arbeit nur die pseudonymisierten Daten.
Der Datenmanager ist für die Verteilung und Nutzung der Daten im Projekt sowie die Durchsetzung der Betroffenenrechte zuständig. Dafür müssen folgende Punkte beachtet werden:

- Alle Empfänger verpflichten sich, den Anweisungen des Datenmanagers Folge zu leisten. Dies kann entweder im Konsortialvertrag oder in einem individuellen Datennutzungsvertrag (vgl. Datennutzungsvertrag) erfolgen.
- Der Datenmanager gibt die erfassten Daten an die Partner weiter. Dabei sollte darauf geachtet werden, dass nur die vom Partner benötigten Daten übergeben werden.
- Jede Weitergabe von Daten an die Partner wird protokolliert, damit der Datenmanager jederzeit die Betroffenenrechte durchsetzen kann.
- Spätestens zum Ende der angegebenen Speicherzeit oder beim einem Widerruf einer Einwilligung informiert der Datenmanager die Partner, welche Daten zu löschen sind.

Von den Betroffenenrechten (vgl. Kapitel 4.d) sind für die Rolle des Datenmanagers besonders das Recht auf Auskunft und das Recht auf Löschung relevant. Will ein Betroffener Auskunft über seine Daten haben, so kann der Datenmanager anhand seiner Unterlagen sofort Auskunft darüber erteilen, wer welche Daten über den Betroffenen erhalten hat. Nach aktueller Rechtsauslegung erscheint es, gerade im Bereich der Forschung ausreichend, den Betroffenen über die Art der Daten, die Empfänger und den Zweck zu informieren. Eine detaillierte Auflistung darüber, welcher Partner mit welchen Verfahren die Daten wie ausgewertet hat, erscheint nicht notwendig.
Geht eine Aufforderung zur Löschung ein bzw. widerruft ein Betroffener seine Einwilligung in die Datenverarbeitung, ermittelt der Datenmanager anhand seiner Einwilligungen das Pseudonym dieser Person. Anschließend übermittelt er das Pseudonym an alle Empfänger der Daten und fordert diese zur Löschung auf. Die Löschung kann dabei nach Treu und Glauben erfolgen. Der Datenmanager fordert die Empfänger also auf, die Daten zu löschen und darf annehmen, dass dies für alle übermittelten Daten und gegebenenfalls erstellte Kopien erfolgt. Er muss nicht in der Lage sein, diese Löschung selbst zu erzwingen oder einen Beweis der Löschung erhalten.

6.b Beispiel kombinierte Informations- und Einwilligungsschrift

Fraunhofer IOSB

FH Bielefeld
University of
Applied Sciences

Kombinierte Informations- und Einwilligungsschrift im Experiment „Smarte Küche“ im Rahmen des Forschungsprojektes PASS

Im Rahmen des durch das Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekts PASS werden Versuchsdaten mit Probanden nach den Vorgaben der Europäischen Datenschutzgrundverordnung (EU-DSGVO) verarbeitet. Dabei werden personenbezogene Daten zum Zweck der Wissenschaft und Forschung erhoben, verarbeitet und genutzt.
Während der Durchführung des Experiments werden zuerst ihre Essensgewohnheiten durch einen Fragebogen erfasst. Danach wird die Interaktion mit einer intelligenten Küche durch verschiedene Sensoren erfasst und die Daten gespeichert. Diese Datenerfassung umfasst die Aufzeichnung des gesamten Versuchsbereichs mit Videokameras. Alle erfassten Daten werden für die weitere Forschung zur Verbesserung intelligenter Küchen benötigt.
Alle erfassten Daten werden vor unerlaubtem Zugriff durch Dritte geschützt, eine Übermittlung in Drittländer erfolgt nicht. Wann immer möglich, werden personenbezogene Daten anonymisiert oder pseudonymisiert.
Die Veröffentlichung von Forschungsergebnissen erfolgt ausschließlich in anonymisierter Form und lässt keinen Rückschluss auf Sie als Person zu.
Da es sich bei PASS um ein Verbundprojekt mit mehreren Partnern handelt, findet eine geteilte Nutzung der Daten im Rahmen des Forschungsprojektes statt. Es ist vorgesehen, die im Experiment erhoben Daten, mit den Projektmitarbeitern folgender Partner gemeinsam zu nutzen:

- Fraunhofer IOSB
- Fachhochschule Bielefeld

Sobald der Forschungszweck es zulässt, werden personenbezogene Daten vernichtet bzw. gelöscht. Eine Löschung erfolgt spätestens zum Projektende Ende 2020.

Ich hatte die Möglichkeit, weitere Fragen zum Experiment und der Datennutzung zu stellen. Ich habe die Antworten verstanden und akzeptiere sie.

Ort, Datum: _____ Unterschrift: _____

Wird von der Experimentleitung ausgefüllt:

Pseudonym:

Ich habe eine Kopie dieser Einverständniserklärung erhalten. Ich erkläre hiermit meine freiwillige Teilnahme an dieser Studie. Ich willige in die Erhebung, Verarbeitung und Nutzung meiner personenbezogenen Daten zum Zweck der Wissenschaft und Forschung nach den Vorgaben und im Umfang der obigen Datenschutzerklärung ein.

Über die oben getroffenen Vereinbarungen hinaus, stimme ich einer Veröffentlichung der von mir erfassten Bild- und Videodaten in wissenschaftlichen Publikationen zu. Mir ist bewusst, dass im Falle eines Widerrufs dieser Einwilligung, bereits erfolgte Veröffentlichungen von diesem Widerruf nicht betroffen sind.

☐ ja ☐ nein

Diese Einwilligung kann jederzeit und ohne Angabe von Gründen für die zukünftige Verarbeitung widerrufen werden, ohne dass Ihnen dadurch Nachteile entstehen. Ihren Widerruf richten Sie bitte an die unten genannte Adresse des Verantwortlichen.

Ort, Datum: _____ Unterschrift: _____

Betroffenenrechte nach EU-DSGVO:
Die DSGVO räumt ihnen umfassende Informations- und Interventionsrechte ein, über die wir sie informieren möchten.

- Recht auf Auskunft (Art. 15 EU-DSGVO)
- Recht auf Berichtigung oder Löschung (Art. 16 EU-DSGVO, Art. 16 EU-DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 EU-DSGVO)
- Recht auf Widerspruch gegen die Verarbeitung (Art. 21 EU-DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 EU-DSGVO)
- Sollten Ihre Betroffenenrechte nicht oder nur unzureichend gewahrt sein, haben Sie ein Beschwerderecht bei ihrem Landesdatenschutzbeauftragten

Kontaktdaten des Verantwortlichen:
Im Sinne der EU-DSGVO ist das Fraunhofer IOSB die verantwortliche Stelle für die Datenverarbeitung. Bitte kontaktieren Sie für die Ausübung ihrer Betroffenenrechte:
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Namen und Kontaktdaten des Projektleiters oder eines definierten Verantwortlichen (evtl. noch Stellvertreter)
Ggf. Funktionsemailadresse wie Datenschutz@Projekt

6.c Datennutzungsvertrag

Datennutzungsvertrag für die Daten des Experiments im Rahmen des Forschungsprojekts PASS

zwischen dem

Fraunhofer IOSB
Fraunhoferstr. 1
66136 Karlsruhe

nachfolgend „Datenprovider“ genannt
und

FH Bielefeld
Interaktion 1
33619 Bielefeld

nachfolgend „Datennutzer“ genannt.

Im Rahmen des durch das Bundesministerium für Bildung und Forschung geförderten Forschungsprojekts PASS sollen Versuchsdaten mit Probanden erhoben und verarbeitet werden. Dabei werden personenbezogene Daten zum Zweck der Wissenschaft und Forschung gemäß den Bestimmungen der Europäischen Datenschutzgrundverordnung (EU-DSGVO) erhoben, verarbeitet und genutzt. Die Probanden haben in die Datennutzung zu Forschungszwecken und der geteilten Nutzung der erfassten Daten durch die Forschungspartner eingewilligt. Eine Datenweitergabe an die Forschungspartner durch den Datenprovider erfolgt in pseudonymisierter Form.

Das Fraunhofer IOSB setzt für die Organisation der Datenweitergabe einen Datenmanager ein. Zum Zeitpunkt der Vertragsschließung ist dies Dr. Max Mustermann (max.mustermann@iosb.fraunhofer.de, 0123 4567 89).
Er ist Ansprechpartner für alle Datennutzer. Weiter ist er zentraler Ansprechpartner für Rückfragen und den eventuellen Widerruf von Einwilligungen der Probanden. Sollte Herr Mustermann diese Funktion nicht mehr wahrnehmen können, wird durch das Fraunhofer IOSB umgehend ein Nachfolger bestimmt und alle Datennutzer informiert.

Dieser Vertrag dient dazu, die Rechte und Pflichten der Datennutzer festzuhalten, die Zugriff auf die erhobenen Daten erhalten.

§1 Betroffene Daten (Anwendungsbereich)

Dieser Vertrag regelt die Nutzung von personenbezogenen Daten im Rahmen des Experiments „Smarte Küche“ im Projekt PASS.
Die Wirkung des Vertrags endet, wenn kein Personenbezug mehr hergestellt werden kann. Dies kann beispielsweise erreicht werden, indem in Videodaten Gesichter und andere identifizierende Merkmale vollständig anonymisiert werden. Insbesondere entfallen in diesem Fall auch die Löschfristen.
Gleichzeitig können (aus den bereitgestellten Rohdaten) abgeleitete Daten weiterhin personenbeziehbar und somit von diesem Vertrag abgedeckt sein. Ein einfaches Beispiel sind Fotos von Gesichtern, die aus den Videodaten extrahiert werden.
Bei Bedarf kann der Datenmanager beraten, ob bestimmte Datensätze personenbezogen sind und wie eine ausreichende Anonymisierung erreicht werden kann.

§2 Datenbereitstellung

Nach Abschluss der Datenerfassung können Datennutzer beim Datenmanager Zugang zu den erfassten Daten beantragen. Dieser Antrag ist formlos und kann mündlich erfolgen. Die Voraussetzung für die Weitergabe der Daten ist:
(1) Die Institution des beantragenden Datennutzers ist als verarbeitende Stelle in der Einwilligung der Probanden aufgeführt.
(2) Der Datennutzer willigt in den vorliegenden Nutzungsvertrag ein.

§3 Art und Umfang der erhaltenen Daten

Bei der Datenerfassung werden folgende Daten über die Probanden erfasst:
- Fragenbogen über die Essensgewohnheiten der Probanden
- Aufzeichnungen des gesamten Versuchsbereichs mit Videokameras

Jeder Proband ist durch ein eindeutiges Pseudonym identifiziert, damit sind dem Probanden die von ihm erfassten Messdaten eindeutig zuzuordnen. Die List der Zuordnung von Pseudonymen zu Namen verleibt beim Datenmanager. Der Datennutzer erhält auf Anfrage Teile oder alle pseudonymen Daten, die er für das Erreichen seines Forschungsziels benötigt.
Daten werden durch den Datenmanager zusammen mit Löschfristen und eventuell vorhandenen individuellen Regelungen bereitgestellt.

§4 Datennutzung

Der Datennutzer verpflichtet sich, die erhaltenen Daten nur zum Zwecke der wissenschaftlichen Forschung im Rahmen des Experiments „Smarte Küche“ im Projekt PASS zu nutzen.
§5 Datensicherheit
Der Datennutzer ist verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Sicherheits- und Schutzanforderungen der EU-DSGVO erfüllt sind. Insbesondere sind die Daten vor unrechtmäßigem Zugriff durch Dritte zu schützen. Im Zweifel lässt sich der Datennutzer durch den Datenmanager über geeignete Maßnahmen beraten.

§6 Veröffentlichung

Veröffentlichungen im Rahmen des Verbundprojekts PASS werden durch den Konsortialvertrag geregelt.
Darüber hinaus gelten erweiterte Regelungen für Forschungsergebnisse die auf den erhaltenen Daten beruhen. Die Veröffentlichung von Forschungsergebnissen in Publikationen oder auf Tagungen erfolgt ausschließlich in anonymisierter Form und lässt keinen Rückschluss auf die Probanden zu.
Ausnahmen sind nur möglich, wenn Probanden in die Veröffentlichung der personenbezogenen Daten eingewilligt haben. Der Datenmanager informiert, wenn eine solche Einwilligung vorliegt.

§6 Widerruf der Einwilligung

Probanden in PASS können ihre Einwilligung in die Datenverarbeitung jederzeit und ohne die Angabe von Gründen widerrufen. In diesen Fall fordert der Datenmanager alle Datennutzer auf, Daten zu einem übermittelten Pseudonym umgehend zu löschen. Dies betrifft auch ggf. aus den übermittelten Daten abgeleitete Daten, wenn sie weiterhin personenbeziehbar sind (vgl. §1).

§8 Speicherdauer

Sobald der Forschungszweck es zulässt, werden personenbezogene Daten gelöscht bzw. anonymisiert. Dies erfolgt spätestens zu den Löschfristen, die zusammen mit den Daten übermittelt werden.

§9 Löschanforderung durch den Datenmanager

Aus besonderen Gründen (Widerruf der Probanden, Löschfristen), kann der Datenmanager eine Löschung von bestimmten oder allen bereitgestellten Daten verlangen. Dieser Löschaufforderung ist umgehend Folge zu leisten und zu bestätigen. Die Löschung erfolgt nach Treu und Glauben. Der Datenmanager führt keine Kontrolle der Löschung durch.

§10 Weitergabe der Daten

Datennutzer dürfen die erhaltenen personenbezogenen Daten nicht an Dritte weitergeben.

§ 11 Wahrnehmung der Betroffenenrechte durch den Datenmanager

Der Datenmanager ist für die Wahrnehmung der Betroffenenrechte der Probanden verantwortlich. Sollten entsprechende Anfragen bei den Datennutzern eingehen, ist der Datenmanager umgehend zu informieren.

Ort, Datum: _____ Unterschrift: _____

6.d Vorschläge für Klauseln

Vereinbarung über die datenschutzrechtliche Verantwortung der Projektpartner

Die Vereinbarung über die datenschutzrechtliche Verantwortung der Projektpartner kann auf zwei ganz unterschiedliche Weisen abgebildet werden. Wenn jeder Partner für seine eigenen Aufgaben im Projekt die Verantwortung übernimmt, könnte die Vereinbarung zur datenschutzrechtlichen Verantwortung im Kooperationsvertrag getroffen werden, Eine gesamtschuldnerische Haftung wäre in diesem Falle ausgeschlossen.
Sofern in Verbundprojekten mehrere Partner in ihren jeweiligen Arbeitspaketen (Teilaufgaben, Studien, Experimenten etc.) personenbezogene Daten verarbeiten, gelten sich als gemeinsam Verantwortliche. Sie haben im gemeinsamen Forschungsantrag die Zwecke und Mittel der Verarbeitung festgelegt und müssen gem. Art. 26 DSGVO eine Vereinbarung über ihre Pflichten gegenüber den betroffenen Personen regeln.

Muster einer Vereinbarung zur datenschutzrechtlichen Verantwortung im Kooperationsvertrag:

- (1) Die Projektpartner führen das Verbundprojekt gemeinsam unter Leitung des koordinierenden Partners XXX durch.
- (2) Die Projektpartner übernehmen die datenschutzrechtliche Verantwortung für ihre jeweiligen Aufgaben in dem Projekt XXX, die im anliegenden Gantt-Chart aufgelistet sind (Anlage 1).
- (3) Innerhalb der eigenen Projektaufgabe trägt der jeweils zuständige Partner die datenschutzrechtliche Verantwortung in dem gesetzlich vorgesehenen Umfang. Er übernimmt alle Verpflichtungen aus der Datenschutz-Grundverordnung, insbesondere die Wahrung der Rechte und Pflichten der betroffenen Personen und die Informationspflichten gem. Art. 13 und 14 DSGVO.
- (4) Weitere gesetzliche Datenschutzregelungen (Bundesdatenschutzgesetz, Landesdatenschutzgesetze, Kirchendatenschutzgesetze etc.), bleiben unberührt.

Dem Kooperationsvertrag müsste ein Gantt-Chart oder eine entsprechende Liste beigefügt werden, woraus erkennbar wird, welcher Projektpartner welche Teilaufgaben erfüllt, um eine eindeutige Verantwortungszuweisung offenzulegen. Die Verantwortlichen erfüllen ihre Informationspflichten und wahren die Rechte der betroffenen Personen innerhalb ihrer jeweiligen Teilaufgabe.
Die Projektpartner können die datenschutzrechtliche Verantwortung auch in einer gesonderten Vereinbarung (außerhalb des Kooperationsvertrags) regeln. Dies ist zu empfehlen, wenn die Projektaufgaben erfordern, dass mehrere Partner gemeinsam bestimmte Teilaufgaben erfüllen und zu diesem Zweck personenbezogene Daten gemeinsam verarbeiten. Sie erfüllen die datenschutzrechtlichen Pflichten gemeinsam und haften gesamtschuldnerisch, falls ein Partner seine Pflichten verletzt.

Muster für eine Vereinbarung zwischen gemeinsam Verantwortlichen in einem Forschungsprojekt (Verbundprojekt) gem. Art. 26 DSGVO

(weitere Einzelheiten vgl. Moos, Datennutzungs- und Datenschutzverträge, 2. Auflage Köln 2018)

Präambel
Die Verbundpartner haben sich [mit Kooperationsvertrag vom (…)] mit dem Ziel zusammengeschlossen, [Ziel des Forschungsprojekts, z.B. Entwicklung eines Sozialen Roboters].
An diesem Forschungsziel orientieren sich die Zwecke der Verarbeitung personenbezogener Daten durch die Verbundpartner.

1. Vertragsgegenstand
1.1. Dieser Vertrag stellt eine Vereinbarung gem. Art. 26 Datenschutzgrundverordnung (DSGVO) zur Regelung der Verarbeitung personenbezogener Daten der folgenden Verbundpartner dar:
[Benennung der Verbundpartner]

1.2 Die Verbundpartner entscheiden gemeinsam über die Zwecke und Mittel der Verarbeitung bestimmter personenbezogener Daten im Verbundprojekt.
Die Verbundpartner fungieren daher im datenschutzrechtlichen Sinne als gemeinsam Verantwortliche im Sinne von Art. 26 in Verbindung mit Art. 4 Nr. 6 DSGVO.
1.3. Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Verbundpartner bei der Durchführung der Zusammenarbeit und konkretisiert insbesondere die Verteilung und Erfüllung der Aufgaben und Pflichten nach anwendbarem Datenschutzrecht (insbesondere der DSGVO) zwischen den Verbundpartnern im Hinblick auf die Datenverarbeitung.

2. Zweck, Mittel und Umfang der Datenverarbeitung
2.1 Die Datenverarbeitung erfolgt entsprechend dem Verarbeitungsverzeichnis (Anlage 2), aus dem sich die Verarbeitungstätigkeiten, Zwecke, Mittel und Umfang ergeben, sowie die Kategorien personenbezogener Daten.
2.2 Die Verbundpartner sind sich einig, dass die Datenverarbeitung ausschließlich in einem Mitgliedstaat der Europäischen Union (EU) stattfindet. Jede Datenübermittlung in ein Drittland muss zwischen den Verbundpartnern abgestimmt werden und darf generell nur dann erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Zusammenarbeit, Zuständigkeit und Verantwortung
3.1 Die Verbundpartner erledigen ihre Teilaufgaben im Forschungsprojekt entsprechend der im Kooperationsvertrag vereinbarten Arbeits- und Zeitplanung (z.B. Gantt-Chart).
3.2 Die personenbezogenen Daten sind in einem strukturierten gängigen und maschinenlesbaren Format zu speichern.
3.3 Vor einer etwaigen Löschung von personenbezogenen Daten sind die anderen Verbundpartner zu informieren; diese können der Löschung aus berechtigten Grund widersprechen, etwa sofern sie eine gesetzliche Aufbewahrungspflicht trifft. Die Aufbewahrungspflicht für Forschungszwecke beträgt 10 Jahre. Die Partner haben ein Protokoll über die Löschung bzw. Vernichtung der Daten zu erstellen.
3.4 Die Verbundpartner haben eigenständig dafür Sorge zu tragen, dass sie sämtliche, in Bezug auf die Daten bestehenden, gesetzlichen Aufbewahrungspflichten einhalten können. Sie haben hierzu (unbeschadet etwaiger anderer Regelungen in dieser Vereinbarung) angemessene Datensicherheitsvorkehrungen (Art. 32 ff. DSGVO) zu treffen. Dies gilt insbesondere im Falle der Beendigung der Zusammenarbeit, z.B. nach Erreichung des Forschungszwecks und/oder Beendigung des Forschungsprojekts.
3.5 Die Verbundpartner sind bezüglich der von ihnen im Projekt übernommenen Aufgaben gemeinsam für die Rechtmäßigkeit aller Verarbeitungen verantwortlich.
oder
3.5 Die Verbundpartner sind bezüglich der von ihnen im Projekt übernommenen Aufgaben jeweils allein für die Rechtmäßigkeit aller Verarbeitungen verantwortlich.
3.6 Die Verbundpartner haben die wesentlichen Inhalte dieser Vereinbarung den Betroffenen entsprechend Art. 26 Abs. 2 Satz 2 DSGVO zur Verfügung zu stellen; die Verbundpartner werden sich auf Inhalt und Formulierung dieser Information verständigen.

4. Information der betroffenen Person

4.1 Jeder Verbundpartner hat die Erfüllung der Informationspflichten nach Art. 13 und 15 DSGVO sicherzustellen.

4.2 Den betroffenen Personen sind die erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung zu stellen.

4.3 (Falls eine Projekt-Website besteht): Die zur Verfügung zu stellenden Informationen sind auf der Website (…) (in von jeder Unterseite leicht und jederzeit erreichbaren Form) zu veröffentlichen.

5. Erfüllung der sonstigen Rechte der betroffenen Personen

5.1 Der Verbundpartner (Verbundpartner mit Kontaktdaten einfügen, z.B. der koordinierende Projektpartner) ist als Anlaufstelle für die Bearbeitung und Beantwortung von Anträgen auf Wahrnehmung der sonstigen nach den Art. 15 ff. DSGVO bestehenden Rechte der betroffenen Personen („Betroffenenrechte") zuständig.

5.2 Ungeachtet der Regelung einer Anlaufstelle können sich betroffene Personen an sämtliche Verbundpartner zwecks Wahrnehmung der ihnen jeweils zustehenden Betroffenenrechte wenden. In einem solchen Fall ist der angerufene Verbundpartner dazu verpflichtet, das Ersuchen eines Betroffenen an die (obige Anlaufstelle) unverzüglich weiterzuleiten.

6. Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen

Die Verbundpartner gewährleisten, alle geeigneten technischen und organisatorischen Maßnahmen so durchzuführen, dass die Datenverarbeitung im Einklang mit den Anforderungen anwendbarer Datenschutzbestimmungen (insbesondere DSGVO) erfolgt und den Schutz der Rechte und Freiheiten der betroffenen Personen gewährleistet (Art. 25 DSGVO).

6. Sicherheit der Verarbeitung (Art. 30 DSGVO)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen die Verbundpartner und ggf. deren Auftragsverarbeiter geeignete technische und organisatorische Maßnehmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO).

8. Vergabe von Auftragsverarbeitung

8.1 Jeder Verbundpartner darf Auftragsverarbeitung nur nach vorheriger schriftlicher Zustimmung der jeweils anderen Verbundpartner vergeben.

8.2 Zur Prüfung einer solchen Zustimmung hat der Verbundpartner, der die Auftragsverarbeitung beabsichtigt, den jeweils anderen Verbundpartnern eine Kopie der abzuschließenden Vereinbarung zur Auftragsvereinbarung zur Verfügung zu stellen.

8.3 Ferner muss der beauftragungswillige Verbundpartner den jeweils anderen Verbundpartnern schriftlich bestätigen, dass er dem Auftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt und sich von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen überzeugt hat. Der Bestätigung ist die Ergebnisdokumentation dieser Überprüfung beizufügen.

8.4 Die Vereinbarung hat den Anforderungen der Art. 28, 29 DSGVO zu entsprechen. Sämtliche Verbundpartner müssen die Vereinbarung als Auftraggeber wirksam abschließen. Jeder Verbundpartner kann sich von einem jeweils anderen Partner vertreten lassen.

8.5 Soll ein außerhalb der EU ansässiger Auftragsverarbeiter eingeschaltet werden, findet 8.2 dieser Vereinbarung Anwendung.

8.6 Personenbezogene Daten dürfen erst nach dem wirksamen Abschluss der Vereinbarung zwischen den Verbundpartnern und dem Auftragsverarbeiter nach Maßgabe der Ziffer 6 dieser Vereinbarung weitergeleitet werden.

8.6 Auftragsverarbeiter sind von dem jeweils beauftragenden Verbundpartner regelmäßig (d.h. mindestens einmal jährlich) in geeigneter Form zu überprüfen. Über diese Prüfung ist ein Prüfungsbericht zu erstellen und den jeweils anderen Verbundpartnern unaufgefordert zur Verfügung zu stellen.

8.8 Die Verbundpartner werden sich je zugestimmter Auftragsverarbeitung über deren jeweilige Durchführung insbesondere hinsichtlich der Weisungserteilung gegenüber dem jeweiligen Auftragsverarbeiter sowie dessen Überprüfung im gegenseitigen Benehmen nach Treu und Glauben verständigen.

9. Vorgehen bei Datenschutzverletzungen

9.1 Der Verbundpartner (Verbundpartner einfügen) ist für die Prüfung und Bearbeitung aller Verletzungen des Schutzes personenbezogener Daten gem. Art. 32 DSGVO einschließlich der Erfüllung aller deshalb etwaig bestehender Meldepflichten gegenüber der zuständigen Aufsichtsbehörde nach Art. 33 DSGVO oder gegenüber betroffenen Personen nach Art. 34 DSGVO zuständig.
9.2 Die Verbundpartner werden jede Verletzung des Schutzes personenbezogener Daten unverzüglich den jeweils anderen Partnern anzeigen und bei einer etwaigen Meldung nach Art. 33, 34 DSGVO sowie einer Aufklärung und Beseitigung von derartigen Verletzungen im Rahmen des Erforderlichen und Zumutbaren mitwirken, insbesondere sämtliche in diesem Zusammenhang relevanten Informationen einander unverzüglich zur Verfügung zu stellen.
9.3 Bevor (Verbundpartner einfügen) eine Meldung nach 9.1 dieser Vereinbarung an eine Aufsichtsbehörde oder eine betroffene Person vornimmt, stimmt er das Vorgehen mit den anderen Verbundpartnern ab.

10. Verschwiegenheitspflichten
Die Verbundpartner haben alle mit der Verarbeitung personenbezogener Daten beschäftigten Personen schriftlich zur Wahrung der Vertraulichkeit im Hinblick auf diese Verarbeitung zu verpflichten.

11. Sonstige Verpflichtungen
11.1 Die Verbundpartner werden die Verarbeitungstätigkeiten in das Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO aufnehmen und dort als ein Verarbeitungsverfahren in gemeinsamer oder alleiniger Verantwortung vermerken.
11.2 Sämtliche Verbundpartner haben sich gegenseitig unverzüglich und vollständig zu informieren, wenn Fehler oder Unregelmäßigkeiten bei der Datenverarbeitung oder Verletzungen von Bestimmungen dieses Vertrages oder des anwendbaren Datenschutzrechtes (insbesondere der DSGVO) festgestellt werden.
11.3 Die Verbundpartner benennen jeweils einen festen Ansprechpartner sowie dessen Stellvertreter für sämtliche datenschutzrechtliche Aufgaben im Forschungsprojekt.
Ansprechpartner für (jeweiliger Verbundpartner) ist (jeweiliger Ansprechpartner) …
11.4 Ein Wechsel in der Person des Ansprechpartners ist den jeweils anderen Verbundpartnern unverzüglich mitzuteilen.
11.5 Die Verbundpartner werden sich bei der Einhaltung der vereinbarten Festlegungen sowie anwendbaren gesetzlichen Datenschutzbestimmungen (insbesondere DSGVO) im Rahmen des Erforderlichen und Zumutbaren gegenseitig unterstützen; hierzu zählen insbesondere
• die Verpflichtung, die jeweils anderen Verbundpartner bei der Etablierung und Aufrechterhaltung angemessener technischer und organisatorischer Maßnahmen gem. Ziff. 6 dieser Vereinbarung zu unterstützen;
• die Verpflichtung, sich gegenseitig bei einer etwaig erforderlichen Datenschutz-Folgenabschätzung und etwaigen Konsultationspflichten der zuständigen Aufsichtsbehörde gem. Art. 35, 36 DSGVO zu unterstützen;
• die Verpflichtung, sich bei der Einrichtung und Pflege der beidseitigen Verzeichnisse der Verarbeitungstätigkeiten zu unterstützen.
11.6 Die Verbundpartner verpflichten sich, alle im Zusammenhang mit diesem Vertrag, der Zusammenarbeit oder der Datenverarbeitung stehenden Maßnahmen und deren Auswirkungen zu dokumentieren.

12. Zusammenarbeit mit Aufsichtsbehörden
12.1 Die Verbundpartner zeigen den jeweils anderen Verbundpartnern an, wenn sich eine Datenschutzaufsichtsbehörde im Zusammenhang mit dieser Vereinbarung, der Zusammenarbeit oder der Datenverarbeitung an sie wendet.
12.2 Die Verbundpartner sind sich darüber einig, dass Aufforderungen zuständiger Datenschutzaufsichtsbehörden grundsätzlich Folge zu leisten ist, insbesondere sind etwaig angeforderte Informationen zu überlassen und die Möglichkeiten zur Prüfung (auch vor Ort) einzuräumen. Die Partner gewähren zuständigen Datenschutzaufsichtsbehörden in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.
12.3 Soweit wie möglich werden sich die Verbundpartner im gegenseitigen Benehmen miteinander abstimmen, bevor etwaige Anfragen von zuständigen Datenschutzaufsichtsbehörde Folge geleistet wird bzw. Informationen im Zusammenhang mit dieser Vereinbarung, der Zusammenarbeit oder der Datenverarbeitung an zuständige Datenschutzaufsichtsbehörden herausgegeben werden.

13. Haftung

13.1 Die Verbundpartner haften gegenüber betroffenen Personen nach den gesetzlichen Vorschriften.

13.2 Die Verbundpartner stellen einander im Innenverhältnis von jeglicher Haftung frei, soweit sie jeweils Anteil an der Verantwortung für die haftungsauslösende Ursache tragen. Das gilt auch im Hinblick auf eine gegen einen Verbundpartner etwa verhängte Geldbuße wegen eines Verstoßes gegen Datenschutzvorschriften mit der Maßgabe, dass die mit der Geldbuße belegten Verbundpartner zunächst die Rechtsmittel gegen den Bußgeldbescheid ausgeschöpft haben muss. Bleibt der jeweilige Verbundpartner danach ganz oder teilweise belastet, die nicht ihrem internen Anteil an der Verantwortung für den Verstoß entspricht, ist der jeweils andere Partner verpflichtet, sie von der Geldbuße in dem Umfang freizustellen, in dem die anderen Partner an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

14.1 Für die Laufzeit und Beendigung der Vereinbarung gelten die Regelungen des Kooperationsvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Verbundpartnern, insbesondere dem Kooperationsvertrag, gehen die Regelungen dieser Vereinbarung vor.

14.2 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Verbundpartner verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 26 DSGVO am besten gerecht wird.

14.3 Es gilt deutsches Recht einschließlich der DSGVO.

Anlage 1: Gantt-Chart (oder Zeit-und Arbeitsplanung zu den Projektaufgaben).
Anlage 2: Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO).

(Unterschriften)

6.e Muster - Eintrag in ein Verfahrensverzeichnis

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	Stand

Verantwortlicher (Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)

Falls zutreffend: Angaben zu weiteren gemeinsam für die Verarbeitung Verantwortlichen (jeweils Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)

Ggf. Datenschutzbeauftragter (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)

Allgemein: Welche Verarbeitungstätigkeiten sind in das Verzeichnis aufzunehmen?

Aufzunehmen sind alle ganz oder teilweise automatisierten Verarbeitungstätigkeiten – also alle Verarbeitungstätigkeiten, die ganz oder teilweise mit Hilfe von IT-Systemen erfolgen.
Nichtautomatisierte Verarbeitungstätigkeiten müssen dann aufgenommen werden, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO).
Ein „Dateisystem" ist nach Art. 4 Nr. 6 DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist. Es spielt dabei keine Rolle, oder die Sammlung zentral oder dezentral vorliegt.
Das Verarbeitungsverzeichnis soll einerseits alle Verarbeitungstätigkeiten ausreichend konkret darstellen, anderseits nicht zu kleinteilig sein. Für ein Forschungsprojekt könnte es sinnvoll sein, folgende beispielhafte Verarbeitungstätigkeiten als eigene Verfahren zu betrachten, die aufgenommen werden müssen:

- Sammlung von möglichen Probanden, die für die Durchführung von Experimenten angeschrieben werden
- Experimente in deren Umfang personenbezogene Daten erhoben und ausgewertet werden
- Register von Personen, die regelmäßig (z.B. über einen Newsletter) über den Projektfortschritt informiert werden

Zu Nr.1 (Allgemeine Angabe)

Namen und Kontaktdaten des Verantwortlichen, ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten (Art. 30 Abs. 1 Satz 2 a DSGVO)
„Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 6 DSGVO). Der Verantwortliche wurde zu Beginn des Forschungsvorhabens festgelegt. Die in Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO genannten „Vertreter" sind in Forschungsprojekten nur relevant, wenn der Verantwortliche nicht in der Europäischen Union niedergelassen ist (Art. 4 Nr. 16 DSGVO).
Gemeinsame Verantwortung für die Verarbeitung liegt vor, wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen (Art. 26 DSGVO). Dies ist beispielsweise der Fall, wenn mehrere Partner in einem Forschungsverbund gemeinsam Experimente durchführen.
Als „Anschrift" ist jeweils Postleitzahl, Ort, Straße und Hausnummer anzugeben.

2. Zwecke und Rechtsgrundlagen der Verarbeitung

Zwecke

Rechtsgrundlagen

Zu Nr.2 (Zwecke und Rechtsgrundlagen)
(Art. 30 Abs. 1 Satz 2 b DSGVO)
Der Zweck sollte so präzise wie möglich sein, meistens geht er direkt aus der Bezeichnung der Verarbeitungstätigkeit hervor. Für das Verzeichnis der möglichen Probanden wäre der Zweck die Rekrutierung von Probanden. Die Rechtsgrundlage ist für die Forschung typischerweise die Einwilligung (Art. 6 Abs. 1 Satz 1 a DSGVO).

3. Kategorien der personenbezogenen Daten

Laufende Nummer	Rechtsgrundlagen

Zu Nr. 3 (Kategorien der personenbezogenen Daten)
(Art. 30 Abs. 1 Satz 2 c DSGVO)
Unter Kategorien sind aussagefähige Oberbegriffe zu verstehen, z.B. „Name und Vorname", „Anschrift", „Staatsangehörigkeit".

4. Kategorien der betroffenen Personen

Laufende Nummer	Rechtsgrundlagen

5. Kategorien der Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

Laufende Nummer	Empfänger	Anlass der Offenlegung

Zu Nr. 5 (Kategorien der Empfänger)
(Art. 30 Abs. 1 Satz 2 d DSGVO)
Nach Art. 4 Nr. 9 DSGVO ist Empfänger „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht". Zu den Empfängern gehören daher auch Auftragsverarbeiter.
Wenn eine gemeinsame Verantwortung vorliegt und Daten im Konsortium geteilt wird, sind die datenempfangenden Partner im Konsortium Empfänger im Sinne der DSGVO, die sind jedoch kein Dritten.

6. Falls zutreffend: Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

Laufende Nummer	Drittland oder Internationale Organisation	Geeignete Garantien im Falle einer Übermittlung nach Art.49 Abs. 1 Unterabsatz z. 2 DSGVO

Zu Nr. 6 (Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation)
(Art. 30 Abs. 1 Satz 2 e DSGVO)
Als Drittländer werden alle Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraumes bezeichnet. Im Falle einer Übermittlung an ein Drittland oder eine internationale Organisation nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO sind die geeigneten Garantien in Bezug auf den Schutz personenbezogener Daten in Spalte 3 festzuhalten. Soweit erforderlich kann dazu auf ergänzende Dokumente verwiesen werden.

7. Vorgesehen Fristen für die Löschung der verschiedenen Datenkategorien

Laufende Nummer	Löschungsfrist

Zu Nr. 7 (Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien)
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke erforderlich ist, für die sie verarbeitet werden (Grundsatz der „Speicherbegrenzung", Art. 5 Abs. 1 e DSGVO). Gespeicherte Daten sind daher unverzüglich zu löschen, sobald sie für die Aufgabenerfüllung nicht mehr erforderlich sind (vgl. DSGVO-Erwägungsgrund 39). Der Verantwortliche sollte daher Fristen für die Löschung oder regelmäßige Überprüfung der personenbezogenen Daten vorsehen (vgl. DSGVO-Erwägungsgrund 39).
Über den eigentlichen Speicherungsanlass hinaus kann eine Speicherung auch zur Erfüllung von Dokumentationspflichten erforderlich sein.

8. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO

Zu Nr. 8 (Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO)
(Art. 30 Abs. 1 Satz 2 g DSGVO)
Hier sind die technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO allgemein zu beschreiben. Trotz der in Art. 30 Abs. 1 Satz 2 g DSGVO verwendeten Formulierung „wenn möglich" hat der Verantwortliche hier in aller Regel Angaben zu machen, da er ohnehin verpflichtet ist, „geeignete technische und organisatorische Maßnahmen" zu treffen. Entsprechende Informationen werden dem Verantwortlichen daher in aller Regel vorliegen.

9. Datenschutz-Folgenabschätzung

Ist für die Form der Verarbeitung eine Datenschutz-Folgeabschätzung nach Art. 35 DSGVO erforderlich?		
☐ Ja	☐ Nein	Falls ja, bis wann durchzuführen oder zu überprüfen:
Begründung		

Zu Nr. 9 (Datenschutz-Folgenabschätzung)
Welches Risiko für die Rechte und Freiheiten natürlicher Personen von einer beabsichtigten Verarbeitung personenbezogener Daten ausgeht und wie dieses Risiko bewältigt werden kann, ist vor jeder Verarbeitung zu prüfen. Eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 Satz 1 DSGVO ist dagegen nur durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge" hat. Diese Voraussetzung liegt regelmäßig vor, wenn besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO verarbeitet werden (z.B. in der Medizinforschung), wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen vorgenommen wird (z.B. Profiling) oder wenn eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche erfolgt.

6.f Checkliste TOM zur Datensicherheit gemäß Art. 32 DSGVO

Projektdaten

Verarbeitungsverfahren	
Verantwortlicher	
Datum	

Regelmäßige Überprüfung

Datum	Ergebnis

Zugangskontrolle

Verhinderung von unbefugtem Zugang zu Verarbeitungsanlagen:

- ☐ Zutrittskontrollsystem
- ☐ Pförtner
- ☐ Alarmanlage
- ☐
- ☐

Datenträgerkontrolle

Verhinderung von unbefugter Verarbeitung von Datenträgern:

- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Vernichtung von nicht mehr benötigten Datenträgern
- ☐
- ☐

Speicherkontrolle

Verhinderung unbefugter Verarbeitung von personenbezogenen Daten:

- ☐ Festlegung von Berechtigungen in den IT-Systemen
- ☐ Verwaltung der Rechte durch Systemadministratoren
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐
- ☐

Benutzerkontrolle

Verhinderung unbefugter Nutzung automatisierter Verarbeitungssysteme:

- ☐ Bedarfsorientiertes Berechtigungskonzepts
- ☐ Regelmäßige Kontrolle von Berechtigungen
- ☐ ständig aktualisierte Berechtigungen
- ☐
- ☐

Zugriffskontrolle

Verhinderung der Nutzung eines Verarbeitungssystems außerhalb des angedachten Zwecks

- ☐ Identifizierung und Authentifizierung der Benutzer
- ☐ Passwortgeschützter Bildschirmschoner
- ☐ Protokollierung von Zugriffen auf Anwendungen
- ☐
- ☐

Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt oder zur Verfügung gestellt werden.

- ☐ Protokollierung der Datenübertragung
- ☐ Netzwerkdokumentation
- ☐ Festlegung der zugelassenen Übermittlungsberechtigten
- ☐
- ☐

Eingabekontrolle

Gewährleistung, dass Nachvollziehbarkeit der Eingabe und Veränderung personenbezogener Daten jederzeit gegeben ist.

- ☐ Identifizierung und Authentifizierung der Nutzer
- ☐ Passwortrichtlinie inkl. Passwortlänge und -wechsel
- ☐ Protokollierung der Änderungen an Daten, Anwendungen und Systemen
- ☐
- ☐

Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

- ☐ Backup und Recoverykonzept
- ☐ Integritätsgeschütze Dateisysteme verwenden
- ☐ Virenscanner
- ☐
- ☐

Transportkontrolle

Gewährleistung, dass personenbezogene Daten bei Übertragung zu jeder Zeit gesichert sind und alle Übermittlungen nachvollziehbar sind.

- ☐ Verschlüsselung von Übertragungen
- ☐ Verschlossener Transport von Datenträgern
- ☐ Nutzung von VPNs zur Datenübertragung
- ☐
- ☐

Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

- ☐ Vertragliche Regelung der Datenverarbeitung
- ☐ Kontrolle und Überwachung
- ☐ Definierte Ansprechpartner und Vertretung
- ☐
- ☐

Wiederherstellbarkeit

Gewährleistung, dass personenbezogene Daten nach einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- ☐ Backup und Recoverykonzept
- ☐ Redundante Datenspeicherung
- ☐ Regelmäßiger Test der Datenwiederherstellung
- ☐
- ☐

Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- ☐ Firewall
- ☐ Virenschutz
- ☐ Notfallkonzept
- ☐
- ☐

Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

- ☐ Redundante Systeme
- ☐ Klimatisierte Räume für IT-Systeme
- ☐ Unterbrechungsfreie Stromversorgung
- ☐ Ausreichende Lagerhaltung von Ersatzteilen
- ☐ Wartungsverträge
- ☐
- ☐

Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:

- ☐ Trennung von Produktiv- und Testsystemen
- ☐ getrennte Datenbanken
- ☐ getrennte Netzbereiche
- ☐ Nutzer- und Rollenkonzept für unterschiedliche Verarbeitungsbereiche
- ☐
- ☐

Raum für Ihre Notizen

Raum für Ihre Notizen

Impressum

Webseite
www.guide-projekt.de

Herausgeber
Dr.-Ing. Erik Krempel und
Prof. Dr. jur. Brunhilde Steckler

Redaktion
Thomas Janicki, Niels Diekmann, Dr.-Ing. Erik Krempel,
Prof. Dr. jur. Brunhilde Steckler, Carolin Lebek

Layout
Carolin Lebek

Druck
WIRmachenDRUCK GmbH
Mühlbachstr. 7
71522 Backnang

Anschrift der Redaktion
Fraunhofer Institut für Optronik, Systemtechnik und
Bildauswertung IOSB
Interaktive Analyse und Diagnose
Fraunhoferstraße 1
76131 Karlsruhe

Bildquellen

Einband: fotolia.com ID: 162241958
Alle anderen Abbildungen:
© Fraunhofer IOSB

Förderung durch das BMBF
Projektträger: VDI/VDE/IT
FKZ: 16SV7890K
Laufzeit: 01.10.2017 bis 31.01.2019

Kontaktdaten

Fachhochschule Bielefeld
Fachbereich Wirtschaft und Gesundheit
Interaktion 1
33619 Bielefeld

Ansprechpartner
Prof. Dr. jur. Brunhilde Steckler
Telefon +49 521 106 5070
steckler@fh-bielefeld.de

Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Abteilung Interaktive Analyse und Diagnose IAD
Fraunhoferstraße 1
76131 Karlsruhe

Ansprechpartner
Dr.-Ing. Erik Krempel
Telefon +49 721 6091 292
erik.krempel@iosb.fraunhofer.de

Fraunhofer IOSB

FH Bielefeld
University of
Applied Sciences