
# Ethik und Datenschutz

05. Juli 2021

**Disclaimer:**

Dieses Dokument wurde im Auftrag der Europäischen Kommission (Generaldirektion Forschung und Innovation) von einem Expertengremium erstellt. Es soll innerhalb der Wissenschaftsgemeinde – insbesondere bei Begünstigten von Forschungs- und Innovationsprojekten der Europäischen Union – eine bewusstseinsfördernde Wirkung entfalten, stellt aber keine offizielle EU-Leitlinie dar. Weder die Europäische Kommission noch eine in ihrem Auftrag handelnde Person können für die Verwendung des Dokuments verantwortlich gemacht werden.

Rechtlicher Hinweis: Dieser Leitfaden begründet für die Europäische Kommission, für Exekutivagenturen oder für Forscher, die eine Ethik-Selbstbewertung vornehmen, keinerlei neue Verpflichtungen.

**Danksagungen:**

Dieses Dokument wurde von dem Experten Ben HAYES und der Mitarbeiterin Albena KUYUMDZHIEVA (DG R&I, derzeit EISMEA) unter Aufsicht des Sektors Forschungsethik und Integrität, Generaldirektion Forschung & Innovation, der Europäischen Kommission verfasst.

Das Dokument wurde mit den Ethikexperten Marjo RAUHALA und James A HOUGHTON abgestimmt.

Der Sektor Forschungsethik und Integrität, Generaldirektion Forschung & Innovation, möchte sich bei allen Beteiligten bedanken.

European Commission
DG Research & Innovation
RTD.03.001- Research Ethics and Integrity Sector
E-mail: RTD-ETHICS-REVIEW-HELPDESK@ec.europa.eu
ORBN
B-1049 Brussels/Belgium

**Übersetzung:**

Diese Übersetzung entstand im Auftrag des Verbundprojektes EcoDM.

DOI: 10.5281/zenodo.6259754

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Förderkennzeichen 16DWWQP

Übersetzungsfirma
Dialecta
Grünberger Str. 26
10245 Berlin

Lektorat und Redaktion
Claus Spiecker
Christine Burkart
Jasper Bothe

## Inhaltsverzeichnis


I. Einleitung ..... 4
II. Identifizierung und Behandlung ethischer Fragen in Ihrem Forschungsvorhaben ..... 7
III. Pseudonymisierung und Anonymisierung ..... 8
IV. Datenschutz durch Technikgestaltung („by design") und Voreinstellungen („by default") ..... 10
V. Informierte Einwilligung in die Datenverarbeitung ..... 11
VI. Erhebung von Daten über Kinder ..... 13
VII. Verwendung zuvor erhobener Daten (‚sekundäre Verwendung') ..... 14
VIII. Datenschutz-Folgenabschätzungen ..... 16
IX. Profiling, Tracking, Überwachung, automatisierte Entscheidungsfindung und Big Data ..... 18
X. Datensicherheit ..... 20
XI. Übermittlung personenbezogener Daten in Nicht-EU-Länder ..... 22
XII. Erhebung personenbezogener Daten außerhalb der Europäischen Union ..... 23
XIII. Löschung und Archivierung von Daten ..... 24
XIV. Datenschutzbeauftragte und andere Anlaufstellen ..... 24

## I. Einleitung

Datenschutz ist für die Forschungsethik in Europa von zentraler Bedeutung und stellt ein grundlegendes Menschenrecht dar. Er ist eng verknüpft mit Autonomie und Menschenwürde und dem Grundsatz, dass jeder geschätzt und respektiert werden sollte. Damit dieser Grundsatz die Entwicklung der heutigen Informationsgesellschaft anleiten kann, muss Datenschutz von der Forschungsgemeinschaft konsequent umgesetzt werden.

Das Recht auf Datenschutz ist in der Charta der Grundrechte der EU und im Vertrag über die Arbeitsweise der Europäischen Union verankert, die dem Recht des Einzelnen auf Schutz der Privatsphäre Wirkung verleihen, indem sie ihm die Kontrolle über die Art und Weise geben, wie Informationen über ihn gesammelt und verwendet werden.[1]

Im Rahmen von Forschungsprojekten sind Forscher datenschutzrechtlich dazu verpflichtet, die Teilnehmer ausführlich darüber zu informieren, was mit den von ihnen gesammelten personenbezogenen Daten geschehen wird. Zudem müssen datenverarbeitende Organisationen sicherstellen, dass alle Daten ordnungsgemäß geschützt und minimiert und nicht mehr benötigte Daten vernichtet werden.

In Abhängigkeit von dem konkreten Umfeld oder den jeweiligen Informationen können sich für die betroffenen Personen verheerende Folgen ergeben, wenn es versäumt wird, personenbezogene Daten vor Verlust oder missbräuchlicher Verwendung zu schützen. Dem Datenverantwortlichen und/oder dem Datenverarbeiter selbst drohen neben einer Schädigung seines Rufes ernsthafte rechtliche und finanzielle Konsequenzen.[2] In der jüngeren Vergangenheit gab es zahlreiche Beispiele für unethische Forschungspraktiken, die eine unbefugte Erhebung und/oder (missbräuchliche) Verwendung personenbezogener Daten beinhalteten und zur Ahndung durch die Aufsichtsbehörden führten.

Während einzelne aus EU-Mitteln finanzierte Forschungsprojekte, in deren Rahmen personenbezogene Daten verarbeitet werden, die datenschutzrechtlichen Bestimmungen der Europäischen Union und der einzelnen Mitgliedstaaten einhalten müssen, soll dieser Leitfaden sicherstellen, dass alle Projekte über die Einhaltung gesetzlicher Pflichten hinaus auch von ethischen Erwägungen und den Werten und Prinzipien, auf denen die EU basiert, geleitet werden.

Spezielle Aufmerksamkeit sollte der Forschung gewidmet werden, die besondere Kategorien von Daten (früher als „sensible Daten" bezeichnet), Profiling, automatisierte Entscheidungsprozesse, Data-Mining-Techniken, die Analyse von Big Data und künstliche Intelligenz mit einschließen, da solche Verarbeitungsvorgänge ein erhöhtes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben können (siehe Tabelle 1). Der wachsende Einfluss dieser und anderer neuer Technologien auf unseren Alltag und unser Leben kommt im Wortlaut und im Geist der EU-Datenschutz-Grundverordnung von 2016 (DSGVO) zum Ausdruck.

Während sich das ethische Begutachtungsverfahren der Europäischen Union in erster Linie mit Ethikfragen befasst, muss Ihr Projekt den Bestimmungen der DSGVO genügen. Die Tatsache, dass ein Forschungsvorhaben rechtlich zulässig ist, bedeutet dabei jedoch nicht zwangsläufig, dass es auch als *ethisch* vertretbar angesehen wird.

Wenn Ihr Forschungsvorhaben mit der Verarbeitung personenbezogener Daten einhergeht, müssen Sie – und alle Ihre Partner, Mitarbeiter und Dienstleister – unabhängig von der angewandten Methode auf Verlangen zwingend die Einhaltung gesetzlicher und ethischer Bestimmungen

---

1 Charta der Grundrechte der Europäischen Union, Artikel 8.

2 Aufsichtsbehörden können Geldbußen von bis zu 20 Mio. € oder 4 % des Gesamtumsatzes des Unternehmens verhängen (je nachdem, welcher Betrag höher ist).

nachweisen können. Dies kann von den betroffenen Personen, von Finanzierungsagenturen oder von Datenschutzaufsichtsbehörden gefordert werden.

Im Rahmen der Ausarbeitung und Umsetzung Ihres Vorhabens obliegt es Ihrer Verantwortung, sich über die einschlägigen gesetzlichen Bestimmungen zu informieren und deren Einhaltung sicherzustellen. Alle EU-Projekte, bei denen personenbezogene Daten über identifizierbare menschliche Untersuchungspersonen verarbeitet werden, unterliegen der DSGVO. Der Grundsatz der Rechenschaftspflicht ist ein zentrales Element der DSGVO und verlangt von den Datenverarbeitenden die Einrichtung und Dokumentation von Prozessen zur Einhaltung des Datenschutzes. Wenn Sie in Ihrem Forschungsantrag, der im Falle einer Finanzierungszusage Bestandteil Ihres Vertrags wird, umfassend auf Fragen des Datenschutzes eingehen, können Sie einen wichtigen Beitrag zur Rechenschaftspflicht über das Projekt leisten.

Beachten Sie, dass außer der DSGVO auch nationale Rechtsvorschriften oder damit verbundene EU-Maßnahmen für Ihr Forschungsvorhaben Anwendung finden können:

- wenn in Ihrem Vorhaben Daten verwendet werden, die von für die Verhinderung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten zuständigen Behörden verarbeitet oder zur Verfügung gestellt werden, kann unter Umständen die Richtlinie (EU) 2016/680 zur Anwendung kommen.
- wenn in Ihrem Projekt personenbezogene Daten verwendet werden, die von elektronischen Netzwerken erzeugt oder verarbeitet werden (z. B. Daten im Zusammenhang mit ‚Cookies', Internetnutzung oder elektronischem Netzwerkverkehr), ist möglicherweise die EU-Datenschutzrichtlinie (derzeit in Überarbeitung) auch anzuwenden.

Die Mitgliedstaaten der Europäischen Union haben eigene Datenverarbeitungsvorschriften erlassen. So können etwa für die Verarbeitung besonderer Kategorien von Daten (wie genetische, biometrische und/oder medizinische Daten) zusätzliche nationale rechtliche Anforderungen wie eine vorherige Benachrichtigung von Aufsichts- oder Datenschutzbehörden gelten. Es liegt in Ihrer Verantwortung, sicherzustellen, dass Ihre Forschung den datenschutzrechtlichen Bestimmungen aller Mitgliedstaaten, in denen Ihre Forschungsdaten verarbeitet werden, und der DSGVO gerecht wird.[3]

[3] Siehe insbesondere Artikel 9(4), 8 und 89(3) DSGVO.

**[Box 1] Schlüsselthemen, Begriffe und Definitionen**

Der Begriff **„Personenbezogene Daten“** ist sehr weit gefasst und beinhaltet **„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen”**. Eine **„identifizierbare natürliche Person”** oder **„betroffene Person”** ist **„eine Person, 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann”** (Artikel 4(1) DSGVO).

Zu personenbezogenen Daten gehören Daten wie Internet-Protokoll (IP)-Adressen (eindeutige Identifikatoren, über die der Besitzer von mit dem Internet verbundenen Geräten identifiziert werden kann) und Daten von „intelligenten Messsystemen” (‚Smart Meters‘), die den Energieverbrauch von Adressen, die mit identifizierbaren Personen verbunden sind, überwachen.

Für **„besondere Kategorien personenbezogener Daten”** (früher als „sensible Daten” bezeichnet) gelten strengere Datenschutzgarantien. Dazu gehören **„Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person”** (Artikel 9(1) DSGVO).

Wenn Ihr Projekt die Verarbeitung besonderer Datenkategorien beinhaltet, erhöht sich die Wahrscheinlichkeit, dass es ernsthafte ethische Fragen aufwirft. Daher müssen Sie die Einbeziehung dieser Art von Daten in Ihr Projekt begründen.

Die Definition von **„Datenverarbeitung”** ist sehr breit gefasst. Sie umfasst **„jeden 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”** (Artikel 4(2) DSGVO).

Wenn bei Ihrem Projekt Daten über identifizierbare Personen eine Rolle spielen, auch wenn diese selbst nicht direkt an der Forschung beteiligt sind, ist mit großer Wahrscheinlichkeit davon auszugehen, dass Sie personenbezogene Daten verarbeiten und sowohl EU-Recht als auch nationale Rechtsvorschriften beachten müssen. Lediglich vollständig und unumkehrbar anonymisierte Daten sind von diesen Anforderungen ausgenommen. Wenngleich auch **Pseudonymisierung** einzelnen betroffenen Personen ein gewisses Maß an Schutz und Anonymität bieten kann, ist zu beachten, dass pseudonymisierte Daten dennoch als personenbezogene Daten gelten, da die betroffene Person re-identifiziert werden kann (siehe unten).

Auch dann, wenn im Rahmen Ihres Projekts lediglich **anonymisierte Daten** Verwendung finden, können die Herkunft oder Beschaffung der Daten erhebliche ethische Fragen aufwerfen.

Aus der DSGVO ergeben sich Pflichten für beide Seiten:

- für den **„Verantwortlichen für Daten (‚data controller‘)”**, der **„allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet”**, als auch
- für den **„Verarbeiter von Daten (‚data processor‘)”**, der **„personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet”**.

Sie müssen sicherstellen, dass alle Partner, Auftragnehmer oder Dienstleister, die in Ihrem Auftrag und in Ihrem Namen Forschungsdaten verarbeiten, die DSGVO und die Ethikstandards von H2020 einhalten. Wenn Sie die Verantwortung für die Verarbeitung personenbezogener Daten, die im Verlauf Ihres Forschungsprojekts erhoben werden, mit anderen Partnern des Konsortiums teilen, kann es sein, dass es **gemeinsame Verantwortliche für Daten** gibt. In diesem Fall müssen Sie und Ihre Partner Ihre jeweiligen Zuständigkeiten darlegen, die für die betroffenen Personen zugänglich ist und ihnen eine einzige Anlaufstelle (‚single point of contact‘) bereitstellen.

## II. Identifizierung und Behandlung ethischer Fragen in Ihrem Forschungsvorhaben

Alle Forschungsvorhaben, die die Verarbeitung personenbezogener Daten beinhalten, müssen Informationen über Datenschutzvorkehrungen in ihrer Vorhabensbeschreibung liefern. Es ist wahrscheinlicher, dass Ihr Projekt mit erhöhten ethischen Risiken verbunden ist, wenn es Folgendes beinhaltet:

- Verarbeitung „besonderer Kategorien" personenbezogener Daten (früher als „sensible Daten" bezeichnet);
- Verarbeitung personenbezogener Daten von Kindern, schutzbedürftigen Personen oder Personen, die ihre Einwilligung zur Teilnahme an der Forschung nicht gegeben haben;
- komplexe Verarbeitungsvorgänge und/oder die Verarbeitung personenbezogener Daten in großem Umfang und/oder die großräumige, systematische Überwachung eines öffentlich zugänglichen Bereiches;
- Datenverarbeitungstechniken, die in die Privatsphäre eingreifen und als Risiko für die Rechte und Freiheiten der Forschungsteilnehmer angesehen werden, oder Techniken, die für eine missbräuchliche Verwendung anfällig sind; und
- Erhebung von Daten außerhalb der EU oder Übermittlung von in der EU erhobenen personenbezogenen Daten in Nicht-EU-Länder.

**[Tabelle 1] Indikatoren für Datenverarbeitungsvorgänge, die mit erhöhten ethischen Risiken verbunden sein können**

| | |
|---|---|
| **Arten von personenbezogenen Daten** | * rassische oder ethnische Herkunft<br>* politische Meinungen, religiöse oder weltanschauliche Überzeugungen<br>* genetische, biometrische oder gesundheitliche Daten<br>* Sexualleben oder sexuelle Orientierung<br>* Mitgliedschaft in einer Gewerkschaft |
| **Betroffene Personen** | * Kinder<br>* schutzbedürftige Personen<br>* Personen, die der Teilnahme am Projekt nicht ausdrücklich zugestimmt haben |
| **Umfang oder Komplexität der Datenverarbeitung** | * umfangreiche Verarbeitung personenbezogener Daten<br>* umfangreiche, systematische Überwachung öffentlich zugänglicher Bereiche<br>* Einbeziehung mehrerer Datensätze und/oder Dienstleister oder Kombination und Analyse verschiedener Datensätze (d. h. Big Data) |
| **Techniken der Datenerhebung oder -verarbeitung** | * in die Privatsphäre eingreifende Methoden oder Technologien (z. B. verdeckte Beobachtung, Überwachung, Tracking oder Täuschung von Personen)<br>* Einsatz von Kamerasystemen zur Überwachung von Verhalten oder zur Erfassung sensibler Informationen<br>* Data Mining (einschließlich der Sammlung von Daten aus sozialen Netzwerken), „Web Crawling" oder Analyse sozialer Netzwerke<br>* Erstellung von Profilen von Einzelpersonen oder Gruppen (insbesondere verhaltensbezogenes oder psychologisches Profiling)<br>* Einsatz künstlicher Intelligenz zur Analyse personenbezogener Daten<br>* Einsatz automatisierter Entscheidungsprozesse, die erhebliche Auswirkungen auf die betroffene(n) Person(en) haben |
| **Beteiligung von Nicht-EU-Ländern** | * Übermittlung personenbezogener Daten in Nicht-EU-Länder<br>* Erhebung personenbezogener Daten außerhalb der EU |

Weitere Indikatoren für die Arten von Projekten und Datenverarbeitungsvorgängen, die als stärker risikobehaftet angesehen werden können, werden im gesamten Leitfaden beschrieben (siehe insbesondere die Abschnitte über Datenschutz-Folgenabschätzungen und über Profiling, Tracking, Überwachung, automatische Entscheidungsfindung und Big Data).

**Wenn Ihre Forschungsarbeit eine stärker risikobehaftete Datenverarbeitung beinhaltet, müssen Sie eine detaillierte Analyse der durch Ihre Projektmethodik aufgeworfenen ethischen Fragen vorlegen.** Diese sollte Folgendes beinhalten:

- eine Übersicht über alle geplanten Datenerhebungs- und Verarbeitungsvorgänge,
- eine Identifizierung und Analyse der ethischen Fragen, die sich daraus ergeben, und
- eine Erläuterung, wie Sie diese Probleme in der Praxis entschärfen wollen.

Sie müssen sicherstellen, dass diese Fragen in dem Forschungsprotokoll, das Sie Ihrer Ethikkommission vorlegen, gebührend berücksichtigt und behandelt werden. Zudem kann es sein, dass Sie eine Datenschutz-Folgenabschätzung (DSFA) gemäß Artikel 35 DSGVO und den ergänzenden DSFA-Richtlinien (siehe unten) vornehmen müssen.

Wenn Ihre Einrichtung einen Datenschutzbeauftragten (DSB) bestimmt hat, sollten Sie diesen in allen Phasen Ihres Projekts einbeziehen und seinen Rat zu Fragen des Datenschutzes einholen. Dies wird Ihnen bei der Umsetzung Ihres Vorhabens und der Finanzhilfevereinbarung (‚Grant Agreement') helfen (EU-Zuwendungen sind an die vollständige Einhaltung der Datenschutzbestimmungen gebunden).

Wenn eine komplexe, sensible oder umfangreiche Datenverarbeitung geplant ist oder Daten in Länder außerhalb der Europäischen Union übermittelt werden sollen, sollten Sie den DSB zur Vereinbarkeit der Datenschutzvorkehrungen mit den Richtlinien der Gasteinrichtung und den geltenden Rechtsvorschriften befragen.

Die Stellungnahme und/oder Empfehlung des DSB sollten Sie in Ihre Vorhabensbeschreibung einfügen. Wenn Ihre Gasteinrichtung nicht über einen Datenschutzbeauftragten verfügt, empfiehlt es sich, einen entsprechend qualifizierten Experten zu Rate zu ziehen.

## III. Pseudonymisierung und Anonymisierung

Eine der besten Möglichkeiten, ethische Bedenken bezüglich der Nutzung personenbezogener Daten zu entkräften, besteht darin, die Daten zu anonymisieren, sodass sie sich nicht mehr auf identifizierbare Personen beziehen. Daten, die keinen Bezug mehr zu identifizierbaren Personen haben, wie etwa aggregierte und statistische Daten oder die auf andere Weise anonymisiert wurden, so dass die betroffenen Personen nicht re-identifiziert werden können, stellen keine personenbezogenen Daten dar, weshalb sie nicht in den Anwendungsbereich des Datenschutzrechts fallen.

Allerdings kann Ihr Forschungsvorhaben auch dann erhebliche ethische Fragen aufwerfen, wenn nur anonymisierte Datensätze verwendet werden sollen. Diese könnten in Zusammenhang mit der Herkunft der Daten oder der Art und Weise, wie sie beschafft wurden, stehen. Aus diesem Grund müssen Sie in Ihrer Vorhabensbeschreibung die Quelle der Datensätze angeben und auf alle sich daraus ergebenden ethischen Fragen eingehen. Zudem müssen Sie die Möglichkeit einer missbräuchlichen Verwendung der Forschungsmethodik oder der Ergebnisse sowie das Schadensrisiko für die Gruppe oder Community prüfen, auf die sich die Daten beziehen.

Wenn ein Bezug der Forschungsteilnehmer zu ihren personenbezogenen Daten erhalten bleiben muss, sollten Sie die Daten nach Möglichkeit pseudonymisieren, um die Privatsphäre der betroffenen

Personen zu schützen und das Risiko einer Gefährdung ihrer Grundrechte im Falle eines unbefugten Zugriffs zu minimieren. Pseudonymisierung und Anonymisierung sind nicht dasselbe und es ist wichtig, dass Sie den Unterschied zwischen ihnen kennen, da Sie diese gemäß DSGVO anwenden müssen, wann immer dies möglich oder machbar ist (Artikel 89 DSGVO).

**[Box 2] Pseudonymisierung und Anonymisierung: den Unterschied verstehen**

Bei **Pseudonymisierung** handelt es sich um den Austausch persönlich identifizierbarer Informationen (z. B. des Namens einer Person) durch eine eindeutige Kennung, die keinen Bezug zur tatsächlichen Identität der Person hat, unter Verwendung von Techniken wie Verschlüsselung oder Hashing. Wenn jedoch die Möglichkeit besteht, betroffene Personen durch eine Umkehr der Pseudonymisierung zu re-identifizieren, müssen die geltenden Datenschutzverpflichtungen weiter beachtet werden. Sie gelten erst dann nicht mehr, wenn die Daten vollständig und unumkehrbar anonymisiert sind.

**Anonymisierung** besteht in der Anwendung von Verfahren, mit deren Hilfe personenbezogene Daten in anonymisierte Daten umgewandelt werden können. Die Anonymisierung stellt eine zunehmende Herausforderung dar, da die Möglichkeit einer Re-Identifizierung besteht.

Bei **Re-Identifizierung** handelt es sich um die Rückumwandlung pseudonymisierter oder anonymisierter Daten in personenbezogene Daten mithilfe von Data Matching oder vergleichbaren Verfahren.

Wenngleich anonymisierte Daten nicht mehr als personenbezogene Daten eingestuft werden, sind Anonymisierungsprozesse mit Herausforderungen verbunden, insbesondere wenn es um große Datensätze mit einem breiten Spektrum an personenbezogenen Daten geht. Das liegt daran, dass es sehr schwierig ist, vollständig anonyme Datensätze zu erstellen, in denen die für Forschungszwecke erforderlichen Detailinformationen erhalten bleiben.[4] Bezogen auf Ihr Forschungsvorhaben bedeutet das, wenn eine große Wahrscheinlichkeit für eine Re-Identifizierung von Personen besteht, deren Daten gesammelt wurden, sollten die Informationen als personenbezogene Daten behandelt werden. Es ist schwer, das Risiko einer Re-Identifikation mit absoluter Sicherheit zu bestimmen, weshalb Sie immer auf Nummer sicher gehen sollten. Eine wachsende Zahl von Fallstudien und Forschungspublikationen, in denen Personen anhand von „anonymen" Datensätzen identifiziert wurden, verdeutlicht die grundlegenden Beschränkungen von Anonymisierung als Verfahren zum Schutz der Privatsphäre von Einzelpersonen.

Wenn Sie die Daten, die Sie für Ihr Forschungsprojekt erheben, anonymisieren möchten, ist das Timing für den Anonymisierungsprozess von zentraler Bedeutung. Sie sammeln nur dann „anonymisierte" Daten, wenn die Anonymisierung zeitgleich mit der Datenerhebung bei der betroffenen Person erfolgt, so dass wirklich keine personenbezogenen Daten verarbeitet werden. Findet die Anonymisierung dagegen zu einem späteren Zeitpunkt statt, indem Sie beispielsweise beabsichtigen, persönlich identifizierbare Informationen bei der Transkription von Audioaufzeichnungen oder bei der Eingabe von Umfragedaten in eine Datenbank zu entfernen, so stellen die Rohdaten nach wie vor personenbezogene Daten dar und Ihre Vorhabensbeschreibung muss Maßnahmen beinhalten, wie die Daten bis zu ihrer Löschung oder Anonymisierung geschützt werden sollen.

Unter Umständen kann Ihre Gast- oder Fördereinrichtung oder Ihr Verlag von Ihnen fordern, dass Sie Rohdaten zu Überprüfungs- oder Rechenschaftszwecken oder zur Sicherstellung der Forschungsintegrität aufbewahren. Denkbar ist auch, dass eine Gasteinrichtung über einen Rohdatensatz verfügt, den sie ihren Forschern und Partnern in anonymisierter Form zur Verfügung stellt. Während die Empfänger der anonymisierten Daten in diesen Fällen von Datenschutzauflagen befreit sein können – sofern das Risiko einer Re-Identifikation minimiert wird – verarbeitet die Gasteinrichtung immer noch personenbezogene Daten und muss daher für einen angemessenen

[4] Siehe auch *Stellungnahme 05/2014 zu Anonymisierungsverfahren*, Artikel-29-Arbeitsgruppe (angenommen am 10. April 2014).

Schutz der (personenbezogenen) Rohdaten sorgen. Dies beinhaltet technische und organisatorische Maßnahmen zum Schutz der Daten und der Wege zur Identifizierung der betroffenen Personen (z. B. der Schlüssel, Codes oder Anwendungen zur Anonymisierung der Daten) gegen unbefugten Zugriff oder Verwendung. Wenn Sie Zweifel haben, ob die Verfahren, die Sie einsetzen wollen, angemessen sind, sollten Sie Ihren DSB oder einen entsprechend qualifizierten Experten um Rat fragen. Wie weiter unten erwähnt (siehe Box 5), kann es bei sensiblen oder komplexen Verarbeitungsvorgängen, die eine Pseudonymisierung oder Anonymisierung beinhalten, sogar erforderlich sein, eine DSFA (Datenschutzfolgenabschätzung) durchzuführen, um ein angemessenes Maß an Datenschutz zu gewährleisten und das Risiko einer Beeinträchtigung der Rechte der betroffenen Personen zu minimieren.

## IV. Datenschutz durch Technikgestaltung („by design") und Voreinstellungen („by default")

Im Interesse ethischer und verantwortungsbewusster Innovationsbemühungen sind Forscher und Entwickler seit langem dazu angehalten, das Konzept „Privatsphäre durch Technikgestaltung" („privacy by design") anzuwenden, das einen Rahmen schafft, um die Gestaltung von Systemen, Datenbanken und Prozessen an der Wahrung der Grundrechte der betroffenen Personen auszurichten. Ein umfassenderes Konzept von „Datenschutz durch Technikgestaltung" („data protection by design"), das jetzt in die DSGVO aufgenommen wurde, verpflichtet die für die Daten Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen zu ergreifen, um den zentralen Datenschutzgrundsätzen der DSGVO Wirkung zu verleihen (Artikel 5 und 25 DSGVO). Datenschutz durch Technikgestaltung stellt einen der besten Ansätze zum Umgang mit ethischen Bedenken dar, die sich aus Ihrem Forschungsvorhaben in der Planungsphase Ihres Projekts ergeben.

Im Kontext von Forschung und Entwicklung könnten Maßnahmen, um Datenschutz durch Technikgestaltung zu verwirklichen, Folgendes enthalten:

- Pseudonymisierung oder Anonymisierung personenbezogener Daten;
- Datenminimierung (siehe Box 3);
- angewandte Kryptographie (z. B. Verschlüsselung und Hashing);
- Inanspruchnahme datenschutzfokussierter Dienstleister und Speicherplattformen; und
- Vorkehrungen, die es den betroffenen Personen ermöglichen ihre Grundrechte wahrzunehmen (z. B. hinsichtlich des direkten Zugangs zu ihren personenbezogenen Daten und der Einwilligung in deren Verwendung oder Übermittlung).

Wenn Sie überlegen, ob und wie Sie den Grundsatz des Datenschutzes durch Technikgestaltung anwenden, sollten Sie

- die Art, den Umfang, den Kontext und den Zweck der Verarbeitung,
- die Schwere der Risiken, die sich für die Grundrechte der betroffenen Personen ergeben, wenn Sie deren Daten nicht schützen, und
- die Kosten und die Verfügbarkeit der Technologien und Anwendungen, die Sie möglicherweise benötigen,

berücksichtigen.

Sie müssen den Grundsatz von Datenschutz durch Technikgestaltung anwenden, wenn dadurch die ethischen Risiken reduziert werden können, die durch die Datenverarbeitung in Ihrem Forschungsprojekt entstehen, und in Ihrem Forschungsantrag erklären, wie dies erreicht werden soll.

Betont wird dieser Ansatz durch den Grundsatz des Datenschutzes durch Voreinstellungen („data

protection by default"). **Wo immer Sie die Möglichkeit haben, Ihren Forschungsteilnehmern ein höheres Maß an Datenschutz zu bieten, sollten Sie solche Maßnahmen standardmäßig anwenden, anstatt sie lediglich in Betracht zu ziehen oder sie als optionale Zusatzleistung zu erbringen.**

Wenn Ihre Forschung komplexe, sensible oder umfangreiche Datenverarbeitungsvorgänge beinhaltet, sollten Sie in Ihrem Antrag beschreiben, welche Maßnahmen Sie ergreifen werden, um die Grundsätze des Datenschutzes durch Technikgestaltung und durch Voreinstellungen anzuwenden und/oder die Sicherheit zu erhöhen, um den unbefugten Zugriff auf personenbezogene Daten oder Geräte zu verhindern.

**[Box 3] Datenminimierung**

Datenverarbeitung muss rechtmäßig, fair und transparent sein. **Es sollten nur Daten erhoben werden, die erforderlich und angemessen sind**, um die spezielle Aufgabe oder den Zweck, zu dem die Erhebung erfolgt, zu verwirklichen (Artikel 5(1) DSGVO).

Aus diesem Grund sollten Sie **nur die Daten erheben, die Sie zur Erreichung Ihrer Forschungsziele benötigen.** Das Sammeln personenbezogener Daten, die Sie für Ihr Forschungsprojekt nicht benötigen, kann als unethisch und ungesetzlich angesehen werden.

Wenn Sie Zweifel haben, ob Sie alle Daten, die Sie zu erheben beabsichtigen, auch tatsächlich benötigen, sollten Sie **eine Datenminimierungsprüfung vornehmen.** Diese sollte von dem Forschungsteam geplant und durchgeführt werden, um sicherzustellen, dass die Daten auf **„Bedarfsbasis"** („**'need-to-know' basis**") gesammelt werden, d. h., dass sie für einen bestimmten relevanten, auf die Ziele und die Methodik Ihres Projekts beschränkten Zweck erforderlich sind.

**Datenminimierung bezieht sich nicht nur die Menge der erhobenen personenbezogenen Daten, sondern auch auf den Umfang, in dem auf sie zugegriffen, sie weiterverarbeitet und/oder weitergegeben werden können, für welche Zwecke sie verwendet werden, und den Zeitraum, für den sie aufbewahrt werden.** Sie müssen die Verarbeitung der Daten auf das mögliche Mindestmaß beschränken.

Wenn Sie den Zweck der Datenverarbeitung zum Zeitpunkt der Erhebung der Daten nicht vollständig bestimmen können oder die Daten über die Dauer Ihres Projekts hinaus aufbewahren müssen, **müssen Sie die Modalitäten der Datenerhebung und -aufbewahrung erläutern und begründen.**

**Zudem müssen Sie erklären, wie Sie die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung in der Praxis anzuwenden gedenken.** Insbesondere müssen Sie sicherstellen, dass

- Sie Daten pseudonymisieren oder anonymisieren, wo immer dies möglich ist (siehe Box 2),
- alle Daten sicher gespeichert werden und
- bei Bedarf Strategien und Verfahren festgelegt werden, um die Verwendung der Daten einzuschränken und die Grundrechte der betroffenen Personen zu wahren.

## V. Informierte Einwilligung in die Datenverarbeitung

Die informierte Einwilligung ist der Eckpfeiler der Forschungsethik. Sie erfordert, dass Sie den Forschungsteilnehmern erklären, worum es bei Ihrer Forschung geht, was ihre Teilnahme an Ihrem Projekt mit sich bringt und alle Risiken, die damit möglicherweise verbunden sein können. Erst wenn Sie diese Informationen an die Teilnehmer weitergegeben haben – und sie sie gänzlich verstanden haben – können Sie deren ausdrückliche Zustimmung zur Mitwirkung bei Ihrem Projekt einholen und in Ihr Projekt einbeziehen (Artikel 4(11) und 7 DSGVO).[5]

[5] Bei Forschungsvorhaben, die klinische Prüfungen beinhalten, sollte die Datenverarbeitung zudem den Bestimmungen der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen von Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG

Grundsätzlich sollten lebende Personen nicht Gegenstand eines Forschungsprojekts sein, ohne darüber informiert zu werden, selbst in den relativ seltenen Fällen, in denen die Forschungsmethoden, -bedingungen oder -ziele vorschreiben, dass sie nicht vor deren Abschluss vollständig über die Art der Studie aufgeklärt werden. Das Aufkommen des Internets und die weit verbreitete Nutzung von Social-Media-Plattformen und anderen IKT (Informations- und Kommunikationstechnologien) haben die Möglichkeiten zur Erforschung menschlichen Verhaltens ohne ausdrückliche Einwilligung der Versuchspersonen jedoch drastisch erweitert. Für die Forschergemeinde ergibt sich dadurch wiederum eine Reihe von ethischen Dilemmata und Herausforderungen.

Wann immer Sie personenbezogene Daten direkt bei Forschungsteilnehmern erheben, müssen Sie im Wege eines Verfahrens, das die Mindeststandards der DSGVO erfüllt, deren informierte Einwilligung einholen. Dies macht es erforderlich, dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgt, mit der eine freiwillig für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Zustimmung der betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten bekundet wird.[6] Dies kann in Form einer schriftlichen Erklärung, die auch auf elektronischem Wege eingeholt werden kann oder in Form einer mündlichen Erklärung erfolgen.

Dieser Prozess sollte nach Möglichkeit in ein umfassenderes Verfahren eingebunden werden, das den in der *Leitlinie zur informierten Einwilligung* der Kommission dargelegten Standards entspricht. Bei Projekten, die besonders komplexe oder sensible Datenverarbeitungsvorgänge oder in die Privatsphäre eingreifende Methoden wie das Erstellen von Verhaltensprofilen, die Anfertigung von Audio-/Videoaufzeichnungen oder die Standortbestimmung beinhalten, sollten Sie jedoch ein die Datenverarbeitungskomponente Ihres Projekts abdeckendes spezielles Verfahren zur informierten Einwilligung implementieren.

Sie müssen Aufzeichnungen machen, die das Einwilligungsverfahren dokumentieren, einschließlich der Informationsblätter und Einwilligungsformulare, die an die Forschungsteilnehmer ausgehändigt wurden, sowie der Einholung ihrer Zustimmung zur Datenverarbeitung. Diese Aufzeichnungen können von den betroffenen Personen, den Finanzierungsagenturen oder den Datenschutzaufsichtsbehörden angefordert werden.

Damit die Einwilligung in die Datenverarbeitung „in Kenntnis der Sachlage“ (‚informed‘) erteilt werden kann, müssen der betroffenen Person detaillierte Informationen über die geplante Datenverarbeitung in verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache gegeben werden. Diese Informationen sollten mindestens Folgendes beinhalten:

- die Identität des für die Datenverarbeitung Verantwortlichen und gegebenenfalls die Kontaktdaten des DSB (Datenschutzbeauftragten),
- den/die konkreten Verarbeitungszweck(e), zu dem die personenbezogenen Daten genutzt werden,
- die Rechte der betroffenen Personen nach der DSGVO und der Charta der Grundrechte der EU, und zwar insbesondere das Recht auf Widerruf der Einwilligung oder auf Einsichtnahme in ihre Daten, die erforderliche Vorgehensweise, sollten sie das wollen, und das Recht auf Einreichung einer Beschwerde bei einer Aufsichtsbehörde,
- Informationen dazu, ob und zu welchen Zwecken die Daten mit Dritten geteilt oder an Dritte übermittelt werden, und
- wie lange die Daten aufbewahrt werden, bevor sie vernichtet werden.

[6] Siehe auch Artikel 7 DSGVO und die *Leitlinien zur Einwilligung gemäß Verordnung 2016/679*, Artikel-29-Arbeitsgruppe (angenommen am 28. November 2017).

Die betroffenen Personen müssen auch darüber informiert werden, wenn die Daten für andere Zwecke genutzt, mit Forschungspartnern geteilt oder an Organisationen außerhalb der EU übermittelt werden sollen (siehe Artikel 13 DSGVO).

Wie bei jedem Forschungsprojekt mit menschlichen Teilnehmern **müssen die betroffenen Personen während des Verfahrens zur informierten Einwilligung auf potenzielle Risiken, die die Datenverarbeitung für ihre Rechte und Freiheiten mit sich bringt, hingewiesen werden.**

Der/die Einwilligungsprozess(e) und die Informationen, die Sie den betroffenen Personen an die Hand geben, sollten alle für die Teilnahme an Ihrem Forschungsprojekt relevanten Datenverarbeitungsaktivitäten abdecken. Wenn Sie beabsichtigen, die Daten dieser Personen für künftige Projekte zu nutzen oder zur Verfügung zu stellen, empfiehlt es sich aus forschungsethischer Sicht und im Einklang mit den Grundsätzen für eine faire und transparente Datenverarbeitung, eine zusätzliche ausdrückliche Einwilligung zur Weiterverwendung der Daten einzuholen[7]. Falls Sie planen, die Daten in mehreren Projekten oder für andere Zwecke als für Ihre Forschung zu verwenden, müssen Sie den betroffenen Personen die Möglichkeit geben, sich gegen die Weiterverarbeitung(en) zu entscheiden.

Falls Sie im Verlauf Ihres Forschungsprojekts wesentliche Änderungen an Ihrer Methode oder den Modalitäten der Datenverarbeitung vornehmen möchten und sich dadurch Auswirkungen auf die Rechte der betroffenen Personen oder die Nutzung ihrer Daten ergeben, müssen Sie diese Personen auf die geplanten Änderungen hinweisen und sie um ihre ausdrückliche Einwilligung bitten. Es genügt nicht, ihnen die Möglichkeit zum Widerspruch einzuräumen. Dies muss geschehen, *bevor* Sie die Änderungen vornehmen.

Wenn Ihr Projekt komplexe und umfangreiche Datenverarbeitungsvorgänge beinhaltet, wenn Sie beabsichtigen, die Daten für mehrere Projekte oder zu verschiedenen Zwecken zu verwenden, oder wenn sich der Zweck der Datenverarbeitung zum Zeitpunkt der Erhebung der Daten nicht vollumfänglich bestimmen lässt, kann es angebracht sein, eine Einwilligungsmanagement-Anwendung zu nutzen. Viele Dienstleister bieten mittlerweile ethisch einwandfreie, sichere Plattformen für eine informierte Einwilligung an, die Ihnen helfen können, Ihren Einwilligungsprozess zu managen, zu dokumentieren und zu belegen.

## VI. Erhebung von Daten über Kinder

Jede Forschung, an der Kinder und Jugendliche beteiligt sind, wirft erhebliche ethische Fragen auf, da

[7] Beispiel: „Eine Forschungsabteilung einer Universität führt ein Experiment durch, in dessen Rahmen an 50 Probanden Stimmungsschwankungen untersucht werden. Hierfür müssen die Probanden ihre Gedanken stündlich zu einer festgesetzten Zeit in einer elektronischen Datei aufzeichnen. Die 50 Personen erteilten ihre Einwilligung zu diesem bestimmten Projekt und zu dieser spezifischen Verwendung der Daten seitens der Universität. Die Forschungsabteilung stellt bald fest, dass die elektronische Aufzeichnung von Gedanken für ein anderes Projekt, das sich mit psychischer Gesundheit befasst und unter der Koordination eines anderen Teams steht, sehr hilfreich wäre. Obgleich die Universität als Verantwortlicher angesichts der miteinander zu vereinbarenden Zwecke dieselben Daten ohne weitere Schritte zur Sicherstellung der Rechtmäßigkeit der Verarbeitung dieser Daten für die Arbeit eines anderen Teams verwenden könnte, setzt sie die Probanden unter Einhaltung ihres Ethikkodex für die Forschung und des Grundsatzes der Verarbeitung nach Treu und Glauben darüber in Kenntnis und bittet sie um deren erneute Einwilligung." (*Handbuch zum europäischen Datenschutzrecht: Ausgabe 2018,* Agentur der Europäischen Union für Grundrechte, Europäischer Gerichtshof für Menschenrechte, Europarat und Europäischer Datenschutzbeauftragter (2018); http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law).

sich diese der Risiken und Folgen ihrer Teilnahme unter Umständen weniger bewusst sind. Dies gilt auch für die Verarbeitung ihrer personenbezogenen Daten.

Wenn im Rahmen Ihres Projekts Daten von Kindern erhoben werden, müssen Sie die *EG-Leitlinie zur informierten Einwilligung* beachten, und zwar insbesondere die Bestimmungen zur Einholung der Einwilligung eines Elternteils/gesetzlichen Vertreters und gegebenenfalls der Zustimmung des Kindes. Wie aus dieser Leitlinie hervorgeht, sind an ein Kind gerichtete Informationen zwingend in einer altersgerechten und einfachen, für das Kind leicht verständlichen Sprache zu formulieren. Zudem müssen Sie auf Forschungsdaten, die Kinder betreffen, den Grundsatz des Datenschutzes durch Technikgestaltung anwenden und die Sammlung und Verarbeitung solcher Daten auf das mögliche Mindestmaß beschränken.

Die DSGVO sieht spezielle Schutzmaßnahmen für Kinder in Bezug auf „Dienste der Informationsgesellschaft" vor, ein weit gefasster Begriff, der alle Internetdienstleister einschließlich Social-Media-Plattformen mit einschließt[8]. Diese beinhalten die Anforderung einer *verifizierten* elterliche Zustimmung, wenn Dienste der Informationsgesellschaft Kindern unter 16 Jahren direkt angeboten werden. Einzelne Mitgliedstaaten können die Altersschwelle auf 13 Jahre herabsetzen. Sofern Sie IKT (Informations- und Kommunikationstechnologien) (z. B. Social-Media-Plattformen oder Apps) nutzen, um Daten von Kindern zu erheben, müssen Sie die nach nationalem Recht und EU-Recht vorgesehenen Schutzmaßnahmen beachten und in Ihrer Vorhabensbeschreibung erläutern, wie Sie die Zustimmung der Eltern/eines gesetzlichen Vertreters einholen und verifizieren werden.

## VII. Verwendung zuvor erhobener Daten (‚sekundäre Verwendung')

Wie oben erwähnt ging es bei einigen der eklatantesten Verstöße gegen Ethikstandards um die Nutzung von Daten, die zu einem bestimmten Zweck erhoben und anschließend ohne Wissen oder Zustimmung der betroffenen Personen für andere Forschungs- oder Targetingprozesse verwendet wurden. Wenn Sie im Rahmen Ihrer Forschung personenbezogene Daten ohne ausdrückliche Einwilligung der betroffenen Personen verarbeiten, müssen Sie erläutern, wie Sie die Daten beschaffen werden, deren Nutzung für Ihr Projekt begründen und sicherstellen, dass die Verarbeitung für die betroffenen Personen fair ist.

Wenn die Erhebung oder Verwendung von Daten besondere ethische Fragen aufwirft (z. B. in Bezug auf Einwilligung und Transparenz, Privatsphäre und die Rechte und Erwartungen der betroffenen Personen), müssen Sie die geplanten Datenerhebungs- und Verarbeitungsvorgänge ausführlich beschreiben und **erläutern, wie den ethischen Bedenken begegnet werden soll.**

Wenn Sie öffentlich verfügbare Daten verwenden, müssen Sie Angaben zu der/den Quelle(n) machen und bestätigen, dass die Daten allgemein und öffentlich zugänglich sind und zu Forschungszwecken genutzt werden dürfen. Dies ist auch dann erforderlich, wenn die Daten, die Sie zu nutzen beabsichtigen, von der betroffenen Person offenkundig veröffentlicht wurden (siehe Box 4).

[8] Siehe auch die Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (Amtsblatt L 241 vom 17.09.2015, S. 1).

**[Box 4] Verwendung von „Open Source"-Daten**

**Die Tatsache, dass manche Daten öffentlich zur Verfügung stehen, bedeutet nicht, dass ihre Verwendung keinen Beschränkungen unterliegt.**

Im Gegenteil, **wenn Sie personenbezogene „Open Source"-Daten über identifizierbare Personen nehmen und neue Datensätze oder Dateien/Profile erstellen, verarbeiten Sie personenbezogene Daten über diese Personen** und Sie müssen eine rechtmäßige/legitime Grundlage haben dies zu tun.

**Sie müssen sicherstellen, dass die Datenverarbeitung für die betroffene Person fair ist und dass ihre Grundrechte gewahrt werden.**

Wenn Sie für Ihr Forschungsprojekt **Daten aus Social-Media-Netzwerken** nutzen und nicht vorhaben, die ausdrückliche Einwilligung der betroffenen Personen zur Verwendung ihrer Daten einzuholen, müssen Sie prüfen, ob diese Personen tatsächlich die Absicht hatten, ihre Informationen öffentlich zu machen (z. B. angesichts der Privatsphäreneinstellungen oder der Bereitstellung der Daten für eine beschränkte Zielgruppe).

Es genügt nicht, dass Daten zugänglich sind; sie müssen so veröffentlicht worden sein, dass die betroffenen Personen keine **begründete Aussicht auf Datenschutz** haben. **Sie müssen auch sicherstellen, dass die von Ihnen geplante Nutzung der Daten allen vom Datenverantwortlichen veröffentlichten Bedingungen und Bestimmungen entspricht.**

Wenn Sie Zweifel haben, was Sie mit dieser Art von Daten tun können und was nicht, sollten Sie sich an Ihren DSB (Datenschutzbeauftragten) oder einen entsprechend qualifizierten Experten wenden und dessen Stellungnahme in Ihre Vorhabensbeschreibung aufnehmen.

Wenn Sie die Absicht haben, personenbezogene Daten zu verwenden, die im Rahmen eines früheren Forschungsprojekts erhoben wurden, müssen Sie Angaben zur ursprünglichen Datenerhebung, zur angewandten Forschungsmethode und zum Verfahren der informierten Einwilligung machen. Zudem müssen Sie bestätigen, dass der Eigentümer/Verwalter der Datensätze Ihnen die Erlaubnis erteilt hat, die Daten für Ihr Projekt zu nutzen.

Stützt sich die geplante Nutzung von Daten auf die „legitimen Interessen" des für die Datenverarbeitung Verantwortlichen, so sind die Art und der Zweck des Datensatzes zusammen mit den Schutzmaßnahmen, die seine Verwendung im Rahmen Ihres Projekts gestatten (z. B. Anonymisierungs- oder Pseudonymisierungsverfahren) detailliert zu beschreiben.[9]

Falls die von Ihnen vorgesehene Datenverarbeitung auf nationalen Rechtsvorschriften oder internationalen Bestimmungen, die Ihre Forschung legitimiert, basiert oder ein nachweisbares, vorrangiges öffentliches Interesse (z. B. die öffentliche Gesundheit oder der soziale Schutz) Ihnen die Nutzung eines bestimmten Datensatzes gestattet, muss Ihre Vorhabensbeschreibung einen Verweis auf die gesetzlichen Bestimmungen oder Richtlinien des betreffenden Mitgliedstaates oder der Europäischen Union enthalten.

Wenn Sie personenbezogene Daten verwenden, die Ihnen ein Dritter zur Verfügung gestellt hat, und die betroffenen Personen deren Nutzung zu Forschungszwecken nicht ausdrücklich zugestimmt haben, sind Sie gemäß DSGVO grundsätzlich verpflichtet, diese Personen darüber zu informieren, dass Sie die Daten eingeholt haben und wofür Sie sie verwenden werden (Art. 14 DSGVO). Zudem müssen sie ihnen die gleichen grundlegenden Informationen über die Datenverarbeitung und ihre Rechte als betroffene Personen zukommen lassen, die auch Personen zur Verfügung zu stellen sind, von denen Sie Daten direkt erheben (siehe Abschnitt V). Diese Anforderungen gelten nur dann nicht,

[9] Gemäß DSGVO kann „[D]ie Rechtmäßigkeit der Verarbeitung durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen". Siehe auch Erwägungsgrund 47 und Artikel 89 DSGVO.

wenn es nicht möglich ist oder einen unverhältnismäßigen Aufwand darstellen würde, die betroffenen Personen zu kontaktieren. In solchen Fällen müssen Sie jedoch geeignete Schutzmaßnahen einschließlich technischer und organisatorischer Maßnahmen treffen, um die Beachtung des Grundsatzes der Datenminimierung (siehe Box 3) sicherzustellen und die Grundrechte der betroffenen Personen zu schützen. Entscheidend ist, dass die DSGVO fordert, dass Pseudonymisierungs- und Anonymisierungsverfahren (siehe oben) anzuwenden sind, wann immer dies praktikabel ist (Artikel 89 DSGVO).

## VIII. Datenschutz-Folgenabschätzungen

Der risikobasierte Datenverarbeitungsansatz, auf dem die DSGVO beruht, kann Forschern mit komplexen, sensiblen oder massenhaften Datenverarbeitungsvorgängen dabei helfen, sich aus ihren Methoden und Zielen ergebende ethische Probleme zu identifizieren und anzugehen.

Die DSFA (Datenschutz-Folgenabschätzung) ist ein Prozess, dessen Zielsetzung darin besteht, die Datenschutzauswirkungen eines Projekts, einer Strategie, eines Programms, eines Produkts oder einer Dienstleistung zu bewerten und in Absprache mit den relevanten Stakeholdern sicherzustellen, dass alle erforderlichen Abhilfe schaffenden Maßnahmen ergriffen werden, um potenzielle negative Auswirkungen für die betroffenen Personen zu korrigieren, zu vermeiden oder zu minimieren.

Nach der DSGVO ist eine DSFA bei Verarbeitungsvorgängen obligatorisch, die „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben" (Artikel 35). Dazu gehören insbesondere:

- eine „systematische und umfassende" Analyse personenbezogener Daten im Rahmen einer automatisierten Verarbeitung, einschließlich Profiling, wenn sich dadurch erhebliche Auswirkungen für die betroffene Person ergeben,
- eine massenhafte Verarbeitung personenbezogener Daten „besonderer Kategorien" oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten oder
- eine systematische Überwachung eines öffentlich zugänglichen Bereiches in großem Umfang.

Die Artikel-29-Arbeitsgruppe der EU (WP29) hat eine längere Liste von Szenarien erstellt, in denen die Durchführung einer DSFA wahrscheinlich erforderlich ist (siehe Box 5). Es wird erwartet, dass der Europäische Datenschutzausschuss und nationale Datenschutzaufsichtsbehörden näher ausführen, für welche Verarbeitungsvorgänge Datenschutz-Folgenabschätzungen obligatorisch sind. Ihrer Verantwortung obliegt es, zu prüfen, ob Sie nach EU-Recht oder nationalem Recht eine DSFA durchführen müssen.

Wenn Ihre Forschungsziele und -methoden eine DSFA gemäß DSGVO erforderlich machen, ist dies in Ihrer Vorhabensbeschreibung zu berücksichtigen. Dabei müssen Sie unter anderem erläutern, wie, wann und von wem die DSFA durchgeführt werden soll.

Sofern aus der DSFA hervorgeht, dass die geplante Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Maßnahmen zur Risikoeindämmung trifft, müssen Sie den Rat Ihrer Datenschutzaufsichtsbehörde dazu einholen, ob die vorgesehene Verarbeitung zulässig ist (Artikel 36 DSGVO). Dies kann wiederum erhebliche Auswirkungen auf die Umsetzbarkeit Ihres Forschungsvorhabens haben und muss daher in Ihrer Risikobewertung berücksichtigt werden.

Falls Sie unsicher sind, ob Sie eine DSFA durchführen müssen, sollten Sie sich an Ihren DSB oder einen entsprechend qualifizierten Experten wenden und dessen Stellungnahme in Ihre Vorhabensbeschreibung aufnehmen. Selbst wenn Sie nicht verpflichtet sind, eine DSFA gemäß der

DSGVO durchzuführen, ist es gute Praxis, eine solche Bewertung vorzunehmen, um das Risiko zu bestimmen und zu minimieren, wenn die vorgesehene Datenverarbeitung komplex, umfangreich oder sensibel ist.

**Unabhängig davon, ob eine DSFA erforderlich ist oder durchgeführt wird, müssen Sie, sofern Ihre geplante Datenerhebung erhebliche ethische Bedenken aufwirft, in ihrer Vorhabensbeschreibung eine sorgfältige Bewertung dieser Risiken vorlegen.** Diese sollte zumindest das Risiko eines unethischen Verhaltens oder einer Beeinträchtigung des Wohlergehens oder der Interessen der Forschungsteilnehmer auf individueller Ebene (z. B. Forschungsteilnehmer, diesen nahestehende Personen oder sonstige Dritte) und auf Gruppenebene (z. B. die Möglichkeit negativer Folgen für die Gemeinschaft, auf die sich die Daten beziehen) beinhalten.

Bei der Beurteilung der aus Ihrem Forschungsvorhaben erwachsenden ethischen Fragen müssen Sie die Gefahr von Diskriminierung, Stigmatisierung und Datenschutzverletzungen (d. h. Offenlegung der Identität oder sensibler Daten einzelner Personen oder Schädigung ihres Rufes durch eine Verletzung der Vertraulichkeit), Bedrohungen für die Sicherheit der Teilnehmer und die Möglichkeit einer missbräuchlichen Verwendung der Forschungsmethode oder der Forschungsergebnisse berücksichtigen.

**[Box 5] Szenarien, in denen Sie eine Datenschutz-Folgenabschätzung vornehmen sollten**

Die WP29 ist der Ansicht, dass **Verarbeitungsvorgänge, die verschiedene datenschutzrechtliche Bedenken aufwerfen, eher ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen können und daher eine DSFA erforderlich machen,** unabhängig davon, welche Maßnahmen der für die Verarbeitung Verantwortliche zu ergreifen beabsichtigt. Der Leitfaden zu Artikel 29[10] nennt folgende Beispiele:

| Beispiele für Verarbeitungsvorgänge | Gegebenenfalls maßgebliche Kriterien | Notwendigkeit einer DSFA wahrscheinlich? |
|---|---|---|
| Ein Krankenhaus verarbeitet die genetischen und gesundheitlichen Daten seiner Patienten (Krankenhausinformationssystem) | - sensible Daten oder Daten mit hohem Personenbezug<br>- Daten zu schutzbedürftigen Betroffenen<br>- Datenverarbeitung in großem Umfang | Ja |
| Ein Kamerasystem wird zur Überwachung des Fahrverhaltens auf Schnellstraßen eingesetzt. Zur Identifizierung einzelner Fahrzeuge und automatischen Erkennung von Nummernschildern plant der für die Verarbeitung Verantwortliche den Einsatz eines intelligenten Videoanalysesystems. | - systematische Überwachung<br>- innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen | Ja |
| Ein Unternehmen überwacht systematisch die Tätigkeiten seiner Angestellten, so auch deren Arbeitsplatzrechner, ihre Internetnutzung usw. | - systematische Überwachung<br>- Daten zu schutzbedürftigen Betroffenen | Ja |
| Aus sozialen Netzwerken werden öffentlich zugängliche Daten erfasst, um daraus Profile zu erstellen. | - Bewerten oder Einstufen<br>- Datenverarbeitung in großem Umfang<br>- Abgleichen oder Zusammenführen von Datensätzen<br>- sensible oder Daten mit hohem Personenbezug | Ja |

[10] *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt",* Artikel-29-Arbeitsgruppe (zuletzt überarbeitet und angenommen am 4. Oktober 2017).

| | | |
|---|---|---|
| Ein Institut erstellt eine Bonitäts- oder Betrugsdatenbank auf nationaler Ebene. | - Bewerten oder Einstufen<br>- automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung<br>- Betroffene Personen werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert<br>- sensible oder Daten mit hohem Personenbezug | Ja |
| Zu Archivierungszwecken werden pseudonymisierte personenbezogene sensible Daten zu schutzbedürftigen Betroffenen gespeichert, die an Forschungsprojekten oder klinischen Studien teilgenommen haben. | - sensible Daten<br>- Daten zu schutzbedürftigen Betroffenen<br>- hindert betroffene Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags | Ja |

## IX. Profiling, Tracking, Überwachung, automatisierte Entscheidungsfindung und Big Data

Die weitverbreitete Nutzung und das große Forschungs- und Entwicklungspotenzial von Informations- und Kommunikationstechnologien haben eine Reihe neuer ethischer Herausforderungen geschaffen. Dazu gehören potenziell nachteilige oder unvorhergesehene Folgen für einzelne betroffene Personen, bestimmte Gemeinschaften und die Gesellschaft als Ganzes. Diese können mit den Auswirkungen der Kombination und Analyse verschiedener Datensätze, der Möglichkeit eines Missbrauchs von Anwendungen oder der Gefahr einer institutionalisierten Diskriminierung zusammenhängen.

**Wenn diese Verfahren bei Ihrem Forschungsprojekt angewandt werden sollen, müssen Sie eine ausführliche Analyse der von Ihrer Methode aufgeworfenen ethischen Fragen vornehmen.** Diese sollte

- einen Überblick über alle geplanten Datenerhebungs- und -verarbeitungsvorgänge,
- eine Identifizierung und Analyse der damit verbundenen ethischen Probleme und
- eine Erläuterung dazu, wie diese Probleme angegangen werden sollen, um sie in der Praxis abzumildern

umfassen.

Wenn bei Ihrem Forschungsvorhaben menschliche Teilnehmer mitwirken, sind solide Verfahren zum Einholen einer informierten Einwilligung erforderlich. **An Ihrem Projekt sind menschliche Teilnehmer beteiligt, wenn Sie diese direkt rekrutieren oder wenn Ihre Forschungsaktivitäten darin bestehen, Personen in irgendeiner Weise aktiv einzubeziehen, zu beeinflussen, zu manipulieren oder zu dirigieren.**

Falls Sie im Rahmen Ihres Projekts eine umfangreiche Verarbeitung personenbezogener Daten mithilfe von Verfahren wie Data Mining, „Web Crawling" oder der Analyse sozialer Netzwerke vornehmen, sollten Sie sowohl den ethischen Auswirkungen der Forschungsmethoden als auch der DSGVO-Konformität der Datenverarbeitung Beachtung schenken.

Sofern das Projekt mit einer automatisierten Verarbeitung oder einem Profiling personenbezogener Daten (siehe Box 6) einhergeht, sollte Ihre Vorhabensbeschreibung die ethischen Auswirkungen der Ziele, Methoden und erwarteten Ergebnisse behandeln. Zudem sind die rechtlichen, gesellschaftlichen

und ethischen Folgen einer Analyse von Big Data zu bedenken,[11] insbesondere deren mögliche Auswirkungen auf das Recht auf Gleichbehandlung und Nichtdiskriminierung.[12]

Wenn Ihr Projekt die Entwicklung oder Nutzung von Technologien beinhaltet, die sich zur Überwachung oder zum Tracking von Personen einsetzen lassen, können diese unter die Dual-Use-Verordnung der Europäischen Union (Verordnung (EG) Nr. 428/2009) fallen oder für eine missbräuchliche Verwendung anfällig sein. In solchen Fällen müssen Sie die Empfehlung der Kommission zu internen Compliance-Programmen für die Kontrolle von Forschung im Zusammenhang mit Gütern mit doppeltem Verwendungszweck und/oder den Leitfaden der Europäischen Kommission über die Möglichkeit des Missbrauchs von Forschungsergebnissen konsultieren.

Falls Ihr Projekt eine intensive Überwachung oder Tracking der Forschungsteilnehmer beinhaltet, z. B. im Hinblick auf ihre Bewegungen, ihr Verhalten, ihre Aktivitäten oder ihre Emotionen, müssen Sie in Ihrer Vorhabensbeschreibung erläutern, welche Maßnahmen ergriffen werden sollen, um ihre personenbezogenen Daten und Grundrechte zu schützen.

Wenn das Projektziel darin besteht, Überwachungstechnologien oder -verfahren für Strafverfolgungszwecke zu entwickeln, sollte Ihre Vorhabensbeschreibung darlegen, warum die Überwachung in einer demokratischen Gesellschaft gemäß den Werten, Prinzipien und Rechtsvorschriften der Europäischen Union für notwendig und angemessen erachtet werden kann.

Wie oben erwähnt kann eine Forschung dieser Art eine DSFA gemäß der DSGVO oder ergänzender Leitlinien von Aufsichtsbehörden erforderlich machen. Wenn Ihre geplanten Forschungsaktivitäten mit vielfältigen oder besonders komplexen ethischen Problemen einhergehen, die in der Antragsphase oder im Rahmen einer anschließenden DSFA nicht gelöst werden können, sollte Ihre Vorhabensbeschreibung eine umfassendere Ethik-Folgenabschätzung vorsehen, die wiederum von Ihrer Forschungsethik-Kommission oder einem sonstigen zuständigen Gremium überprüft werden sollte.

---

11 Siehe auch *Leitlinien für den Schutz von Personen bei der Verarbeitung personenbezogener Daten im Zeitalter von Big Data (Big-Data-Leitlinien), Europarat (Januar 2017)*

12 Charta der Grundrechte der Europäischen Union, Artikel 21

**[Box 6] Automatisierte Datenverarbeitung und Profiling**

Die DSGVO enthält spezielle Schutzmaßnahmen für Vorgänge der automatisierten Verarbeitung oder des „Profilings" personenbezogener Daten, die schwerwiegende rechtliche oder materielle Auswirkungen auf die betroffenen Personen haben oder haben könnten (Artikel 22 DSGVO). Profiling und seine Folgen hängen explizit mit Bewertung und Einstufung zusammen: **Je mehr Profiling in die Privatsphäre eingreift und je größer die potenziellen Auswirkungen des Ergebnisses sind, desto wahrscheinlicher ist es, dass erhebliche ethische und grundrechtliche Fragen aufgeworfen werden.** Die Schutzmaßnahmen der DSGVO sollen betroffene Personen in die Lage versetzen,

- zu verstehen, dass sie einem Profiling unterzogen werden,
- die Logik hinter der Verarbeitung und alle voraussichtlichen Folgen einer solchen Verarbeitung zu kennen,
- der Datenverarbeitung zu widersprechen oder sie zu verweigern und
- die getroffene automatisierte Entscheidung anzufechten oder das Eingreifen einer Person zu erwirken.

Da es sich um Forschungs- und Entwicklungsprojekte (und nicht um konkrete Anwendungen) handelt, haben Ihre Aktivitäten möglicherweise keine wesentlichen rechtlichen oder materiellen Folgen für die betroffene Person. Nach den Grundsätzen des Datenschutzes durch Technikgestaltung und einer verantwortungsbewussten Forschung und Innovation **müssen Sie in der Projektentwicklungsphase jedoch die nach der DSGVO vorgeschriebenen Schutzmaßnahmen für automatisierte Verarbeitungsvorgänge und Profiling beachten.** Wenn Sie beabsichtigen oder erwarten, dass Ihre Methode in einem breiteren Rahmen (z. B. in einem Produkt-, Anwendungs- oder Forschungskontext) angewandt wird, müssen Sie die erforderlichen Schutzmaßnahmen umsetzen.

Zu den Schutzmaßnahmen für Profiling gehören die Anwendung bewährter und zuverlässiger mathematischer und statistischer Methoden, Methoden zur Sicherstellung einer möglichst großen Datengenauigkeit und die Entwicklung von Modellen und Verfahren zur Minimierung des Risikos von Fehlern oder benachteiligenden Auswirkungen. **Transparenz und Rechenschaft gegenüber Forschungsteilnehmern sind von besonderer Bedeutung** und darüber hinaus verlangt die DSGVO von Ihnen, **dass Sie die betroffenen Personen mit Informationen über automatisierte Datenverarbeitungsvorgänge, Profilerstellung und Bewertung versorgen und ihnen die Möglichkeit einräumen, eine Erklärung zu verlangen und die getroffene Entscheidung anzufechten.**

## X. Datensicherheit

Wann und wie auch immer Sie personenbezogene Daten erheben, Sie sind sowohl ethisch als auch rechtlich dazu verpflichtet, sicherzustellen, dass die Informationen der Teilnehmer angemessen geschützt werden. Dies ist von grundlegender Bedeutung, um ihre Rechte und Freiheiten zu wahren und die mit der Datenverarbeitung verbundenen ethischen Risiken zu minimieren.

Die DSGVO sieht vor, dass alle Verantwortlichen für und Verarbeiter von Daten geeignete technische und organisatorische Maßnahmen ergreifen müssen, um ein Maß an Datensicherheit zu gewährleisten, das den Risiken, denen die betroffenen Personen im Falle eines unbefugten Zugriffs, einer Offenlegung, einer versehentlichen Löschung oder einer Vernichtung ihrer Daten ausgesetzt sind, angemessen ist (Art. 32 DSGVO).

In Ihrer Vorhabensbeschreibung sollten Sie die technischen und organisatorischen Maßnahmen, die zum Schutz der bei dem Projekt verarbeiteten personenbezogenen Daten ergriffen werden sollen, näher beschreiben und beispielsweise auf die Datenschutz- und Informationssicherheitsrichtlinien Ihrer Gasteinrichtung und Ihrer Forschungspartner verweisen. Solche Maßnahmen können etwa die Pseudonymisierung und Verschlüsselung personenbezogener Daten sowie Richtlinien und Verfahren zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit von

Verarbeitungssystemen umfassen.

Wenn mit einer stärker risikobehafteten Datenverarbeitung (z. B. im Falle besonderer Kategorien oder umfangreicher Daten) zu rechnen ist, sollten Sie ausführlich erläutern, wie ein erhöhtes Maß an Datensicherheit gewährleistet werden soll. Bei diesen Szenarien kommt es darauf an, dass Sie geeignete Forschungsmethoden und Datenverarbeitungstools auswählen (siehe Box 7).

Unabdingbar ist dies, sobald an Ihrem Projekt Forschungsteilnehmer mitwirken, die schutzbedürftig sind oder aufgrund ihrer Teilnahme schutzbedürftig werden könnten. Dies kann z. B. der Fall sein, wenn Sie Daten zu politisch heiklen Themen erheben oder mit Menschen in autoritär regierten Ländern kommunizieren. Nahezu jede Form von Kommunikation kann überwacht und abgefangen werden, wobei einige Kanäle anfälliger sind als andere. Wo immer Sie vermuten, dass ein erhöhtes Risiko für Forscher und Forschungsteilnehmer besteht, sollten Sie sicherstellen, dass Ihr Informationsaustausch vor einem unbefugten Zugriff sicher ist.

**[Box 7] Datensicherheit: 10 Ge- und Verbote**

Gebote

- ✓ Nutzen Sie DSGVO-konforme Mittel, um personenbezogene Daten von Forschungsteilnehmern zu erheben, zu verarbeiten und zu speichern.
- ✓ Nehmen Sie die Kommunikationssicherheit ernst, entwickeln und implementieren Sie die für Ihr Projekt erforderlichen speziellen Protokolle.
- ✓ Prüfen Sie die Geschäftsbedingungen aller Dienstleister, die Sie im Rahmen Ihres Projekts zur Verarbeitung personenbezogener Daten in Anspruch nehmen (Software, Anwendungen, Speicherung usw.), um Risiken für die betroffenen Personen zu identifizieren und abzumildern.
- ✓ Verschlüsseln Sie Ihre Forschungsdaten und/oder die Geräte, auf denen diese gespeichert werden, und stellen Sie sicher, dass die Schlüssel/Passwörter entsprechend geschützt sind.
- ✓ Fragen Sie Ihren DSB (Datenschutzbeauftragten) oder einen entsprechend qualifizierten Experten, wie Sie ein Maß an Datensicherheit erreichen können, das den Risiken der betroffenen Personen angemessen ist.

Verbote

- ✗ Daten auf einem persönlichen Gerät wie einem Smartphone sammeln, ohne sicherzustellen, dass sie angemessen geschützt sind (berücksichtigen Sie beispielsweise die Auswirkungen automatischer Backups auf die Cloud und die Sicherheitsfunktionen des Gerätes).
- ✗ Kostenlose Dienste in Anspruch nehmen, die möglicherweise die Daten Ihrer Teilnehmer für eigene Zwecke nutzen, anstatt auf kostenpflichtige Dienste zurückzugreifen, oder über soziale Netzwerkplattformen Daten sammeln oder mit Forschungsteilnehmern kommunizieren, ohne zuvor die Auswirkungen auf den Datenschutz zu prüfen.
- ✗ Unverschlüsselte E-Mails, SMS-Nachrichten oder unsichere „Voice over IP"-Plattformen nutzen, um mit schutzbedürftigen oder möglicherweise unter staatlicher Überwachung stehenden Teilnehmern zu kommunizieren.
- ✗ Personenbezogene Daten beim Fernzugriff dem Risiko eines unbefugten Zugriffs oder einer unbefugten Nutzung aussetzen (beispielsweise durch die Nutzung unsicherer WiFi-Verbindungen) oder in Länder reisen, in denen Ihre Geräte durchsucht oder beschlagnahmt werden könnten.
- ✗ Davon ausgehen, dass Ihre Forschungspartner, Mitarbeiter oder Dienstleister über angemessene Richtlinien für Informationssicherheit und Datenschutz verfügen, ohne sich zu vergewissern, dass dies wirklich der Fall ist.

## XI. Übermittlung personenbezogener Daten in Nicht-EU-Länder

Die Übermittlung personenbezogener Daten von Forschungsteilnehmern an Partner, Mitarbeiter oder Dienstleister in Ländern außerhalb der EU wirft ethische und rechtliche Fragen auf, die in der Praxis schwierig zu lösen sind. Außerhalb der EU ansässige Forscher können anderen Ethikregeln unterliegen und ihr Umgang mit den Daten entspricht möglicherweise nicht den EU-Standards.

Nur wenige Nicht-EU-Länder haben einen „Angemessenheitsbeschluss" der Europäischen Kommission erhalten, die bescheinigt, dass sie über einen datenschutzrechtlichen Rahmen verfügen, der ein dem nach EU-Recht vorgesehenen Schutzniveau entsprechendes Maß an Datenschutz bietet.[13]. Dies bedeutet, dass die Daten Ihrer Forschungsteilnehmer unter Umständen keinen angemessenen Schutz erfahren oder sogar auf eine Art und Weise genutzt werden können, die ihre Grundrechte verletzt. Die EU verlangt die Anwendung ihrer Ethikstandards auf alle von ihr finanzierten Forschungsarbeiten, unabhängig davon, in welchem Land sie stattfinden. Für die Übermittlung personenbezogener Daten aus Nicht-EU-Ländern gelten strenge Datenschutzanforderungen nach Kapitel V DSGVO.

Sie **müssen die Daten nicht tatsächlich an ein Nicht-EU-Land „senden", damit diese Bestimmungen anzuwenden sind.** Wenn einer Ihrer Partner oder Dienstleister außerhalb der EU ansässig ist und auf die von Ihnen erhobenen personenbezogenen Daten zugreifen kann, stellt dies bereits eine „Datenübermittlung" im Sinne der DSGVO dar. Ihre Vorhabensbeschreibung muss Angaben zu allen geplanten Datenübermittlungen in Nicht-EU-Länder enthalten. Zudem müssen Sie sicherstellen, dass die Empfänger der Daten das gleiche Datenschutzniveau gewährleisten, das nach europäischem Recht erforderlich ist.

Damit Datenübermittlungen in Nicht-EU-Länder rechtmäßig sind, muss eine der folgenden Voraussetzungen gegeben sein:

- die ausdrückliche Einwilligung der betroffenen Person (was erfordert, dass sie im Voraus über eine solche Datenübermittlung informiert wird);
- ein „Angemessenheitsbeschluss" der Europäischen Kommission in Bezug auf das betreffende Land;
- eine Datenübermittlungsvereinbarung mit EG-Standardvertragsklauseln, die die Anwendung des EU-Datenschutzrechts begründet;
- gemeinsame interne Vorschriften, die sowohl für den Sender als auch für den Empfänger der Daten verbindlich sind und von einer nationalen Aufsichtsbehörde genehmigt wurden.

Diese Anforderungen gelten unabhängig von der Sensibilität der Daten für jede Übermittlung personenbezogener Daten.

Aus forschungsethischer Sicht sollten Daten von Forschungsteilnehmern grundsätzlich nur mit deren informierter Einwilligung in Nicht-EU-Länder übermittelt werden, die gemäß den oben beschriebenen Leitlinien anzufordern ist und eingeholt werden muss.

Wenn Sie in Ihrer Vorhabensbeschreibung die Möglichkeit in Betracht ziehen, dass personenbezogene Daten ohne ausdrückliche Einwilligung der Forschungsteilnehmer in Nicht-EU-Länder übermittelt werden, ist die Rechtsgrundlage für eine solchen Transfer darzulegen. In diesem Fall sollten Sie den Rat des DSB (Datenschutzbeauftragten) Ihrer Gasteinrichtung zur Rechtmäßigkeit der Datenübermittlung einholen und seine Stellungnahme in die Vorhabensbeschreibung aufnehmen. Wenn Ihre Gasteinrichtung nicht über einen DSB verfügt, empfiehlt es sich, einen entsprechend

[13] Die Liste der Länder, für die ein Angemessenheitsbeschluss der Kommission vorliegt, ist unter dem folgenden Link abrufbar: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy- protection-personal-data-non-eu-countries_en

qualifizierten Experten zu konsultieren.

## XII. Erhebung personenbezogener Daten außerhalb der Europäischen Union

Die Erhebung personenbezogener Daten von Forschungsteilnehmern in Nicht-EU-Ländern wirft ähnliche ethische Fragen auf, die jedoch noch dadurch vergrößert werden, dass sichergestellt werden muss, dass die Teilnehmer:

- sich damit wohlfühlen, an einem Forschungsprojekt mitzuwirken, das von Forschern außerhalb ihres eigenen Landes durchgeführt wird,
- sich darüber im Klaren sind, was mit ihren Daten geschehen wird, und
- nicht in unangemessener Weise zur Teilnahme gedrängt werden.

Wie oben erwähnt, gelten die Ethikregeln der EU für alle von der EU finanzierten Forschungsvorhaben, unabhängig davon wo sie stattfinden. In gleicher Weise ist die DSGVO unabhängig vom Ort der Datenverarbeitung auf alle Verarbeitungsvorgänge anzuwenden, die von in der Europäischen Union ansässigen Auftragsverarbeitern durchgeführt werden. Dies bedeutet, dass Sie auch dann, wenn Sie personenbezogene Daten außerhalb der EU erheben, die Einhaltung des EU-Rechts sicherstellen und nachweisen können müssen.

Zudem sind die gesetzlichen Bestimmungen des Landes, in dem Sie Ihre Forschung durchführen, zu beachten, einschließlich aller nationalen Datenschutzgesetze. So kann es beispielsweise erforderlich sein, nationale Behörden oder Datenschutzaufsichtsstellen zu informieren oder deren Erlaubnis für Ihre Forschung einzuholen. Weitere Genehmigungen werden möglicherweise benötigt, um personenbezogene Daten außerhalb des Landes, in dem das Forschungsvorhaben stattfindet, zu übermitteln. Vorschriften zur Datensouveränität können sogar eine Übermittlung von bestimmten Informationen wie Gesundheits- oder Patientendaten aus dem Land heraus verbieten.

Es obliegt Ihrer Verantwortung, zu prüfen, welche gesetzlichen Pflichten für die Forschungsvorhaben, die sie außerhalb der EU durchführen, gelten und alle zu deren Erfüllung erforderlichen Maßnahmen zu ergreifen. Sie müssen zudem in der Lage sein, die Einhaltung der Vorschriften auf Verlangen nachzuweisen. Auch hier gilt: Bei Unklarheiten zu Fragen im Zusammenhang mit internationalen Datenübermittlungen sollten Sie wieder den Datenschutzbeauftragten Ihrer Gasteinrichtung oder einen entsprechend qualifizierten Experten zu Rate ziehen und dessen Stellungnahme in Ihre Vorhabensbeschreibung aufnehmen.

**[Box 8] Checkliste: Internationale Datenübermittlungen**

Übermittlung personenbezogener Daten außerhalb der EU

- ✓ Stellen Sie sicher, dass internationale Datenübermittlungen mindestens eine der in Kapitel V DSGVO beschriebenen relevanten Bedingungen erfüllen.
- ✓ Vergewissern Sie sich, dass alle Drittanbietern, deren Dienste Sie in Anspruch nehmen möchten (z. B. Umfragetools, Datenanalysen, Cloud-Speicher), ihren Sitz in einem EU-Mitgliedstaat haben oder gemäß der DSGVO in der EU rechtmäßig vertreten sind.
- ✓ Treffen Sie mit Partnern oder Dienstleistern rechtlich verbindliche und durchsetzbare Vereinbarungen, bevor Daten übermittelt werden.
- ✓ Verhindern Sie die Weiterleitung personenbezogener Daten durch Mitglieder Ihres Konsortiums und andere Empfänger außerhalb des Rahmens solcher Vereinbarungen.
- ✓ Ergreifen Sie geeignete organisatorische und technische Maßnahmen, um zu gewährleisten, dass personen-bezogene Daten sicher übermittelt werden.

Erhebung personenbezogener Daten in Nicht-EU-Ländern

- ✓ Stellen Sie sicher, dass Bestimmungen zu Verarbeitung, Mitteilung, Einwilligung und Rechenschaftspflicht den DSGVO-Standards entsprechen.
- ✓ Ermitteln Sie alle weiteren Datenschutzanforderungen nach dem geltenden Recht des Landes, in dem Daten erhoben werden sollen, und erläutern Sie in Ihrer Vorhabensbeschreibung, wie Sie diese Bestimmungen umsetzen wollen.
- ✓ Stellen Sie gegebenenfalls sicher, dass die Forschungsteilnehmer die Übermittlung ihrer personenbezogenen Daten in einen EU-Mitgliedstaat oder ein Nicht-EU-Land verstehen und ihr zustimmen.
- ✓ Verwenden Sie Pseudonymisierungs- und Anonymisierungsverfahren, um das Risiko für die betroffenen Personen zu minimieren.
- ✓ Ergreifen Sie geeignete organisatorische und technische Maßnahmen, um zu gewährleisten, dass personenbezogene Daten sicher übermittelt werden.

## XIII. Löschung und Archivierung von Daten

Sie dürfen von Ihnen erhobene personenbezogene Daten nur so lange aufbewahren, wie dies für die Zwecke, zu denen die Daten gesammelt wurden, erforderlich ist oder wie die für das Projekt geltenden Überprüfungs-, Archivierungs- oder Aufbewahrungsbestimmungen dies vorsehen. Diese Bestimmungen sind den Forschungsteilnehmern im Rahmen eines Verfahrens zur informierten Einwilligung zu erläutern.

Jüngere aufsehenerregende Fälle einer missbräuchlichen Nutzung personenbezogener Daten waren darauf zurückzuführen, dass die Verantwortlichen für die Datenverarbeitung es versäumt haben, die Daten zu löschen und Dritte, an die die Daten übermittelt wurden, nach Maßgabe der vereinbarten Nutzungsbedingungen ebenfalls zur Löschung anzuhalten.

Sobald Ihre Forschungsdaten nicht mehr benötigt werden oder der festgelegte Aufbewahrungszeitraum abgelaufen ist, müssen Sie alle Daten sicher löschen und dafür sorgen, dass sie nicht wiederhergestellt werden können.

Zu Überprüfungszwecken aufbewahrte Daten sind sicher zu speichern und ausschließlich für diese Zwecke weiterzuverarbeiten.

Wenn Sie Forschungsdaten in der Cloud oder bei einem Drittdienstleister gespeichert haben, sollten Sie darauf achten, dass die Daten einschließlich aller Backups sicher gelöscht wurden. Wenn im Verlauf des Projekts Daten an Partner oder Dritte weitergeleitet wurden, müssen Sie sicherstellen, dass diese die Daten gelöscht haben, sofern diese keine rechtmäßige Grundlage für ihre Aufbewahrung haben.

## XIV. Datenschutzbeauftragte und andere Anlaufstellen

Wenn Ihre Einrichtung einen DSB (Datenschutzbeauftragten) benannt hat, empfiehlt es sich, dessen Rat dazu einzuholen, worin Ihre Datenschutzpflichten bestehen und wie diese zu erfüllen sind. Sie müssen sicherstellen, dass die Kontaktdaten des DSB allen an Ihrer Forschung beteiligten Personen zugänglich gemacht werden.

Sofern Ihr Projekt aufgrund der Sensibilität der Daten oder des Umfangs bzw. der Art der erforderlichen Verarbeitungsmaßnahmen komplexe Datenschutzfragen aufwirft, sollten Sie es in Betracht ziehen, einen Datenschutzexperten/-berater in Ihren Projekt- oder Forschungsethikausschuss zu berufen. Falls Ihre Gasteinrichtung nicht über einen DSB verfügt, sollten Sie bei der Ausarbeitung

Ihres Vorhabens den Rat eines entsprechend qualifizierten Experten einholen und/oder gegebenenfalls einen solchen Experten für Ihr Projekt benennen.

Wenn Sie Hilfe und Rat im Zusammenhang mit allgemeineren Ethikfragen, die die im Rahmen Ihres Projekts vorgesehene Datenverarbeitung aufwirft, benötigen, wenden Sie sich am besten an die zuständigen institutionellen Einrichtungen oder Dienste (z. B. Forschungsbüro, Forschungsethikausschuss usw.) Ihrer Universität oder Einrichtung, an die zuständigen nationalen Stellen, an die Mitglieder Ihres Konsortiums oder an Kollegen innerhalb Ihres persönlichen Netzwerks, die über einschlägiges Fachwissen und Erfahrung verfügen.

Falls Sie bezüglich einzelner mit Ihrer Forschung verbundener Ethikaspekte Unklarheiten haben, kann es sich anbieten, einen Ethikberater zu ernennen oder einen Ethikmentor zu engagieren, der Ratschläge erteilt, die mit dem Forschungsvorhaben verbundenen ethischen Bedenken im Blick behält und dafür sorgt, dass das Projekt in allen Punkten ethikkonform ist.

Der Ethik- und Datenschutz-Entscheidungsbaum kann Ihnen eine zusätzliche Hilfestellung bieten, um die mit der Projektdatenverarbeitung einhergehenden möglichen Ethikprobleme zu identifizieren und zu beheben.