Handreichung: Upload von nicht-wissenschaftlichen und wissenschaftlichen Videos

Produziert von FIZ Karlsruhe im Rahmen von NFDI4Culture.
Inhalt: Oliver Vettermann

Diese Handreichung entstand im Rahmen des DFG-geförderten Forschungsprojektes NFDI4culture, Projektnummer 441958017.

Präambel

Dieses Dokument dient dazu, die rechtlichen Rahmenbedingungen für den Video-Upload in öffentlich zugänglichen Videoportalen – wie das AV-Portal der TIB Hannover oder YouTube – zu erläutern. **Es ersetzt keine Rechtsberatung und ist kein Dokument für den rechtlichen Gebrauch.** Etwaige Änderungen in rechtlichen Dokumenten (z. B. Lizenzvereinbarungen und Datenschutzerklärungen) sind eigenständig umzusetzen. Im Übrigen erhebt diese Handreichung keinen Anspruch auf Vollständigkeit.

Einführung

Dieses Dokument bietet einen Überblick über datenschutzrechtliche Aspekte beim Upload von Vortragsaufzeichnungen auf kommerziellen oder wissenschaftlichen Video-Plattformen. Besondere Berücksichtigung finden dabei die Unterscheidung zwischen wissenschaftlichen und nicht-wissenschaftlichen Inhalten und die Weiterleitung von Daten in Form des Videos in Drittländer (z. B. USA). Für den umfangreichen Datenschutz-Teil liegt ein Flowchart zum Datenschutz bei Video-Uploads zur Orientierung bei und dient als Checkliste für die einzelnen Punkte, die in diesem Dokument vertieft werden.

Zur Erläuterung der datenschutzrechtlichen Aspekte wird sich den folgenden Beispielen bedient, die zwei unterschiedliche Konstellationen eröffnen: **Beispiel 1** bildet die unmittelbare Bindung zwischen Forscher:in und Video-Dienstleister ab. **Beispiel 2** bindet eine vermittelnde Stelle ein und wird im Verlauf der Handreichung zeigen, dass die vermittelnde Instanz nur einen Teil der Verpflichtungen auffangen kann.

Beispiel 1: Individuelle Forschung

Eine Forscher:in lädt den eigenen Vortrag auf YouTube hoch. Trotz einem Schriftstück über eine Auftragsverarbeitung entspricht der Upload, der nur mit einem entsprechenden Kanal möglich ist, einer gemeinsamen Verantwortlichkeit – hier besteht eine Parametrisierung der Zuschauer:innen, s. o. Die Forscher:in ist damit unmittelbar datenschutzrechtlich Verantwortliche im Rahmen des eigenen YouTube-Kanals.

Beispiel 2: Konsortiale Forschung

Die Forscher:in wendet sich an ein Forschungskonsortium, das einen Kanal auf einem unabhängigen Video-Portal betreibt. Datenschutzrechtlich verantwortlich ist die Forscher:in nicht für den Kanal oder die Statistiken des Videos. Dies obliegt allein dem Forschungskonsortium als gemeinsam Verantwortliche. Hier besteht die gemeinsame Verantwortlichkeit u.a. darin, welche Parameter im Backend des Kanals eingesehen werden können oder welches unabhängige Portal genutzt wird – es können auch verschiedene Portale für jede Wissenschafts-Community genutzt werden. Für diesen Fall sollten die Einzelheiten aber in einer Vereinbarung zwischen Video-Portal und Mittlerin festgehalten werden.

Die datenschutzrechtliche Aufklärung ist in den genannten Beispielen nötig, weil es sich bei den Informationen zu den Teilnehmer:innen oder Vortragenden um personenbezogene Daten handelt. Weitere ergeben sich ggf. aus dem Vortragsinhalt, z. B. wenn über die Vita gesprochen wird.

Abstimmen von Vereinbarungsdokument und Webangebot

Grundlage für die Aufzeichnung und digitale Verwertung einer Konferenz oder sonstigen Veranstaltung ist die rechtliche Absicherung der Aufzeichnungen der Konferenzteilnehmer:innen. Die Datenschutzvereinbarung zur Veranstaltung und die der Webseite bzw. des Video-Portals müssen deshalb inhaltlich aufeinander abgestimmt sein. Dies bedeutet, dass die getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Nutzer:innen und des Angebots (Art. 25, 32 DSGVO) auf dem aktuellen Stand sein müssen. Die Maßnahmen sind auch in Zukunft auf aktuellem Stand zu halten, ggf. durch effektivere auszutauschen.

Bei der Nutzung von Video-Diensten sind als Veranstalter bzw. Uploader alle Verarbeitungstätigkeiten, die nicht im Zusammenhang mit der Video-Angebot selbst stehen – z. B. **Reichweitenmessung oder Marketing-Tools** – so minimalistisch wie möglich zu halten. Wenn möglich, sind sie durch eine geeignete Auswahl der Plattform zu meiden. Andernfalls sind diese Tools so einzustellen (wenn möglich), dass Daten ausreichend anonymisiert sind oder zumindest eine pseudonyme Nutzung möglich ist. Für Pseudonyme gilt die DSGVO und das Datenschutzrecht weiterhin. Deshalb bedarf es einer Verarbeitungsgrundlage sowie der Erfüllung datenschutzrechtlicher Informationspflichten. Werden Daten anonymisiert, ist zumindest die Überführung von personenbezogenen zu anonymisierten Daten zu rechtfertigen, d.h. eine Verarbeitung anzuzeigen, ausreichend zu informieren und eine Rechtsgrundlage bereitzuhalten.

Wird für die **Verarbeitung anonymisierter Daten** eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) genutzt, muss diese aktiv (also Opt-In) erklärt werden. Ein Opt-Out-iFrame und das aktive Deaktivieren sind unzulässig. Das Widerrufen der Einwilligung muss mindestens so leicht möglich sein wie die Einwilligung selbst. Stützt sich die Verarbeitung auf ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) braucht es eine stichhaltige Begründung. Es reicht nicht aus, dass die Verarbeitung „für das eigene Angebot wichtig“ ist oder der „Verbesserung des Dienstes“ gilt. Hier braucht es konkrete Gründe, die eine Verknüpfung zwischen der Erhebung durch das gewählte Tool und die eigene Dienstleistung für Nutzer:innen spürbar sind. Diese

müssen auch in dokumentierter Form mit den Interessen der Nutzenden abgewogen werden. Beispielsweise sind technisch notwendige Session Cookies bei Online-Shops unvermeidbar, weil diese während einer Session die Verbindung mit dem Warenkorb herstellen oder ggf. für einen gewissen Zeitraum eine Wiederherstellung ermöglichen (ähnlich § 25 TTDSG).

Achtung bei der **Anonymisierung von Nutzungsdaten**: Eine Maskierung der IP-Adresse reicht nur dann aus, wenn eine Profilbildung nicht z. B. über damit verbundene Cookies, Tracking-Pixel und ähnliche Profiling- oder Targeting-Methoden möglich ist. Denn dann bleibt die DSGVO weiterhin anwendbar. Daten sind erst dann anonym, wenn sie unter Einbeziehung allen subjektiven Wissens (im Unternehmen) und bei Hinzuziehen üblicher Informationsquellen Dritter (z. B. Forschungspartner aus Konsortien; statistische Informationen der Plattform) auch anonym bleiben. Es kommt also auf den Einzelfall an.

Allgemeine Hinweise zu Datenschutzerklärungen

Portale, die Video-Inhalte (also „audiovisuelle Medien“) zur Verfügung stellen, verarbeiten als Webseite stets **personenbezogene Daten** – zumindest IP-Adressen (bis zur Pseudonymisierung/Anonymisierung) und Cookies (je nach Inhalt bzw. Umfang) auf Seiten der Nutzer:innen. Hinzu kommen personenbezogene Daten vortragender Personen in den Videos selbst, die in vertraglichen Vereinbarungen berücksichtigt werden müssen. Als personenbezogene Daten kommen hier beispielsweise Aussehen und Stimme der Person, Anwesenheit auf Konferenzen oder Informationen, die sich aus dem Hintergrund einer Videokonferenz-Aufzeichnung schlussfolgern lassen. Informationen, die Aussagen über den Gesundheitszustand der Person enthalten – z. B. die Brille als Ausdruck einer Sehschwäche – stellen **besondere personenbezogene Daten** dar. Für die jeweiligen Datenarten müssen also Hinweise und die Zuweisung von Verpflichtungen vorgesehen werden. Daraus sind auch Voraussetzungen abzuleiten, die das Video erfüllen muss. Beispielsweise dürften Aufzeichnungen über Videokonferenz-Programme nicht ohne ausgeblendeten Hintergrund oder die Videosignale der anderen Teilnehmer:innen (z. B. Publikum) hochgeladen werden, ohne dass eine Einwilligung dieser vorliegt. Die bloße Anwesenheit auf einer Konferenz ist jedenfalls keine hinreichende Einwilligung, weil sie nicht freiwillig ist und ihr keine echte Wahl abgesehen von dem Fernbleiben einer Veranstaltung vorausgeht.

Nachfolgend wird auf die jeweiligen, zu beachtenden Punkte eingegangen. Dabei wird allerdings zwischen wissenschaftlichen und nicht-wissenschaftlichen Inhalten der Videos unterschieden. Grund dafür ist die unterschiedliche Rechtsgrundlage für die Verarbeitung der Videobilder von Forscher:innen. Beiden gemein ist allerdings, dass Lizenzvereinbarung und datenschutzrechtliche Einwilligung getrennt voneinander abgefragt werden sollten. Entweder geschieht dies über zwei einzelne Dokumente mit unterschiedlicher Übertitelung oder ein gemeinsames Dokument, das durch Trennungszeichen die Änderung des Erklärungsinhaltes erkennen lässt – z. B. Trennstrich, Überschrift, etc. Wichtig ist, dass mit einem Dokument bzw. einer Einwilligung nicht gleichzeitig zwei rechtliche Zwecke abgefragt werden. Es muss ggf. möglich sein, den Lizenzbedingungen auch ohne eine Datenverarbeitung über den Lizenzvertragszweck hinaus zustimmen zu können. **Konkret: Eine Aufzeichnung sollte auch ohne den Upload möglich sein.**

Datenschutzerklärungen für wissenschaftliche Inhalte

Vorab: Was sind wissenschaftliche Inhalte?

Der Begriff der wissenschaftlichen Inhalte ergibt sich aus dem Zusammenspiel der Art. 89 und 85 DSGVO. Hier verwendet die DSGVO die Begriffe der „wissenschaftlichen Forschungszwecke“ (Art. 89 Abs. 2 DSGVO) und der „Meinungsäußerung und Informationsfreiheit [...] zu wissenschaftlichen Zwecken“ (Art. 85 Abs. 1, 2 DSGVO). In beiden Fällen meint „Wissenschaft“ aber den ernsthaften und planmäßigen Versuch zur Ermittlung der Wahrheit. Wissenschaft wird dabei als Prozess begriffen, der einem stetigen Wandel an Methoden und Einflüssen auf die Ergebnisfindung unterliegt. Es kommt deshalb nicht darauf an, ob „richtige“ Methoden verwendet oder diese vollständig und in richtiger Reihenfolge angewendet wurden. Wichtig ist nur, dass diese systematisch und mit dem Ziel/Zweck einer Antwort auf die aufgestellte Forschungsfrage oder -hypothese eingesetzt werden. Ausgenommen vom Wissenschaftsbegriff ist die Politisierung wissenschaftlicher Aussagen für gesellschaftliche oder ideologische Zielsetzungen. Dies ist eher als Anwendung der Ergebnisse zu sehen, die nicht mehr dem Findungsprozess unterliegt.

Wissenschaftliche Inhalte sind damit all jene Inhalte, die sich mit dem Prozess, Zwischenergebnissen oder dem Ergebnis selbst auseinandersetzen. Dabei können sich die Inhalte auf zwei Unterbegriffe der Wissenschaft aufspalten: Forschung und Lehre. **Forschung** meint die Erkenntnissuche selbst und die Anwendung der methodischen/ wissenschaftlichen Werkzeuge dabei. Dies ist von den „wissenschaftlichen Forschungszwecken“ des Art. 89 Abs. 2 DSGVO gedeckt. Die Kommunikation des Prozesses oder von (Teil-)Ergebnissen in der Öffentlichkeit ist dagegen eine wissenschaftsbezogene Meinungsäußerung, die Teil von Art. 85 Abs. 1, 2 DSGVO ist. In diesen Bereich fällt insbesondere die **Lehre**, die zwar die Forschungsmethoden und -werkzeuge erläutert, aber zugleich Meinungen der lehrenden Person enthalten kann.

Videos mit wissenschaftlichen Inhalten stellen daher, ähnlich wie die Lehre, eine Kommunikation über Methoden, (Teil-)Ergebnisse oder den Forschungsprozess selbst dar. Sie zeichnen sich gerade dadurch aus, dass sie auf einen „work in progress“ zurückgreifen oder unter Bezug auf den Forschungsprozess selbst das Ergebnis (z. B. Thesen, empirische Befunde, etc.) näher erläutern.

Verantwortliche Stellen und andere Beteiligte

Zuerst ist zu klären, in welchem (rechtlichen) Verhältnis die einzelnen Beteiligten zueinander stehen. Je nachdem verteilt sich die Erfüllung datenschutzrechtlicher Pflichten anders. Es sind Konstellationen denkbar, in denen:

- Forscher:in und Video-Portal direkt eine Vereinbarung miteinander schließen *oder*
- zwischen Forscher:in und Video-Portal noch eine Forschungsinstitution als archivierende oder kuratierende Institution eingesetzt ist; sie fungiert gewissermaßen als vermittelnde Stelle.

Die DSGVO trennt zwischen verantwortlichen Stellen und auftragsverarbeitenden Stellen. Als **verantwortliche Stelle** wird jede natürliche oder juristische Person, Behörde, Einrichtung

oder andere Stelle bezeichnet, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Entscheidet sie gemeinsam mit anderen Stellen, kommt eine **gemeinsame Verantwortlichkeit** in Betracht. Die Kontrolle über das Ob und Wie der Verarbeitung liegt bei diesen Stellen. Die **auftragsverarbeitende Stelle** ist das Gegenstück hierzu: Personenbezogene Daten werden im Auftrag einer (gemeinsam) verantwortlichen Stelle verarbeitet. Damit fehlt es an einer Kontrolle und Entscheidung über das Ob und Wie der Verarbeitung; dieses obliegt allein der beauftragenden Stelle.

Problematisch ist bis heute die Differenzierung, ob es sich sowohl im normalen (also Forscher:in – Video-Portal) als auch im Mittler-Verhältnis um eine Auftragsverarbeitung oder gemeinsame Verantwortlichkeit handelt. Dies ist besonders dann zu klären, wenn das Video-Portal statistische Daten entsprechend aufbereitet, also personenbezogene Daten verarbeitet, und diese wiederum auf dem hochgeladenen Video basieren. Dies nimmt unmittelbar Einfluss auf die Verpflichtung der Akteure. Die Unterscheidung ist deshalb wichtig, weil datenschutzrechtliche Pflichten, die Erfüllung von Informationsansprüchen und auch die Haftung der Beteiligten untereinander jeweils anders ausfällt. Es ist deshalb genau **im Einzelfall** zu prüfen, wie bestehende Dokumente/Vereinbarungen oder die tatsächliche Ausführung ausfallen und entsprechend zu deuten sind. Sind diese Dokumente nicht vorhanden, empfiehlt es sich, diese zu erstellen und so das Verhältnis zu klären und abzusichern. Eine Grundlage hierfür kann der Mustervertrag zur Datennutzung von KonsortSWD sein. Basierend auf aktueller Rechtsprechung können folgende Kriterien für eine Einordnung herangezogen werden:

- Die Festlegung der Zwecke der Verarbeitung werden gemeinsam festgelegt. Dabei spielt es keine Rolle, ob diese inhaltlich deckungsgleich sind. Es reicht aus, wenn diese aufeinander aufbauen oder sich gegenseitig fördern (Win-Win-Situation) – selbst, wenn sie in unterschiedliche Richtungen weisen.
- Die jeweiligen Zwecke können nicht unabhängig voneinander erfüllt werden. Eher hängen die Ergebnisse/Verarbeitungen eines Akteurs von denen eines anderen ab.
- Die Akteure entscheiden teilweise oder gänzlich gemeinsam über die (technischen) Mittel der Verarbeitung – z. B. Algorithmen, gewählte APIs, usw. In diesem Bereich sind sie in der Entscheidung frei.
- Es kommt **nicht** darauf an, wie die Erfüllung (datenschutzrechtlicher) Pflichten zwischen den Beteiligten verteilt ist.

Beachte: Die Übergänge sind fließend. Im Zweifel nimmt der Europäische Gerichtshof bislang eine gemeinsame Verantwortlichkeit an, auch wenn die Win-Win-Situation nur entfernt denkbar ist.

Im **direkten Verhältnis zwischen Forscher:in und Video-Portal (Beispiel 1)** sind die vertraglichen Vereinbarungen maßgebend. Ausgehend davon, dass eine Parametrisierung der Abrufzahlen und/oder des Verhaltens der Nutzer:innen (z. B. Pausierung, Springen zu späterer Stelle, etc.) möglich ist, sollte von einer gemeinsamen Verantwortlichkeit ausgegangen werden. Dies ist vor allem dann der Fall, wenn mit dem Upload eines Videos die Verwaltung eines eigenen Video-Kanals zusammenhängt. Dann wirkt das Video-Portal zwar wie ein bloßer Infrastruktur-Anbieter. Der Upload und das (ggf. wiederholte) Zuführen

von Inhalten fördert jedoch die Abrufzahlen des Portals; umgekehrt dient die Reichweite oder die Reputation des Portals den Kanalbetreibenden. Damit ist die erwähnte Win-Win-Situation ausreichend gegeben.

Das **Mittler-Verhältnis (Beispiel 2)** aus Forscher:in, vermittelnder Institution (nachfolgend Mittlerin) und Video-Portal ist da komplexer: Hier besteht die Lizenzvereinbarung sowie Datenschutz-Vereinbarung nur zwischen Forscher:in und Mittlerin. Die Forscher:in gibt hier jedoch nur Rechte ab, erhält im Gegenzug dafür Reichweite/Reputation. Die Kanalverwaltung übernimmt dagegen die Mittlerin; ebenso hat sie die eigenen datenschutzrechtlichen Rechte/Pflichten sowie die des Video-Portals an die Forscher:in weiterzureichen. Damit erscheinen Mittlerin und Video-Portal als gemeinsam verantwortliche Stellen gegenüber der Forscher:in. Die Mittlerin kann hier jede Art verantwortlicher Stellen sein – also entweder eine einzelne verantwortliche Stelle oder ein Konsortium als gemeinsam verantwortliche Stellen. In jedem Fall empfiehlt es sich hier, im Verhältnis der gemeinsamen Verantwortlichkeit zwischen Video-Portal und Mittlerin ein Schriftstück mit den jeweiligen Rechten und Pflichten aufzusetzen, da die allgemeinen Nutzungsbedingungen dies regelmäßig nicht abdecken. Dabei ist die gesamtschuldnerische Haftung des Art. 82 Abs. 4, 5 DSGVO besonders zu berücksichtigen.

Verarbeitungsgrundlagen gem. Art. 6 und 9 DSGVO

Unabhängig von der Verantwortlichkeit bleibt jeweils zu klären, auf welche Rechtsgrundlage die Datenverarbeitung gestützt wird. Gesetzliche Grundlagen bilden zunächst Art. 6 Abs. 1 und 9 Abs. 2 DSGVO. Dieses Dokument bezieht sich ausschließlich auf die in der Regel aufkommenden Verarbeitungsgründe, namentlich die Einwilligung (Art. 6 Abs. 1 lit. a, 7 DSGVO), das Vertragsverhältnis mit der Plattform (Art. 6 Abs. 1 lit. b DSGVO) und das berechtigte Interesse der verarbeitenden Institutionen (Art. 6 Abs. 1 lit. f DSGVO). Spezielle Interessen aus dem Archivrecht werden ausgeklammert.

Hinweis: Besondere personenbezogene Daten, Art. 9 Abs. 1 DSGVO

Vor der Erläuterung geeigneter Verarbeitungsgründe des Art. 6 Abs. 1 DSGVO bedarf es noch eines kurzen Exkurses über besondere personenbezogene Daten. Hierunter sind alle personenbezogenen Datensätze zu verstehen, die aufgrund ihres Inhalts entsprechend sensibel sind, also ein höheres Gefährdungsrisiko haben. Konkret: Informationen über „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“. Ein besonderes Augenmerk liegt bei Konferenzaufzeichnungen regelmäßig auf sichtbaren körperlichen Beeinträchtigungen. Unter dem Stichwort „**Gesundheitsdaten**“ sind insofern die Eigenschaft der Brillenträger:in, Sprachbehinderungen oder andere sicht-, hör- und wahrnehmbare Beeinträchtigungen einzuordnen. Diese offenbaren den aktuellen oder chronischen Gesundheitszustand einer Person; Aufzeichnungen manifestieren also Gesundheitsdaten.

Der Transparenz halber sollte in einem vorhergehenden Aufklärungsdokument (z. B. zur Einwilligung in die Aufzeichnung) auch darauf hingewiesen werden, dass unvermeidlich auch diese Informationen erkennbar sind bzw. verarbeitet werden. Zwar liegt auf diesen regelmäßig

kein Fokus der beteiligten Institutionen. Dennoch hilft der Hinweis dabei, die Grundlage der Verarbeitung vorzubereiten und im Zweifelsfall vorweisen zu können. So liegt über diese Details mit einem unterzeichneten Dokument auch eine Einwilligung vor; hilfsweise stützt die Verarbeitung der Information die Ausnahme des Art. 9 Abs. 2 lit. h DSGVO, nach der die betroffene Person die Information „offensichtlich öffentlich" gemacht hat. Die vorherige Information und die Vortragshandlung selbst wirken so gemeinsam als Verarbeitungsgrundlage.

Einwilligung, Art. 6 Abs. 1 lit. a, 7 DSGVO

Die häufigste gewählte Verarbeitungsgrundlage ist die Einwilligung einer betroffenen Person für „einen oder mehrere bestimmte Zwecke". Sie bietet damit den größtmöglichen Spielraum im Vergleich zu übrigen Grundlagen des Art. 6 Abs. 1 DSGVO. Geltung entfaltet sie jedoch nur zwischen den betroffenen Parteien selbst, also z. B. zwischen Konferenzteilnehmer:in und aufzeichnender Institution als Mittlerin; weitere Institutionen können nur mittelbar je nach Verantwortlichkeit eingebunden werden. Sie muss **freiwillig, in informierter Weise und unmissverständlich** abgegeben werden. Das Einverständnis mit der Verarbeitung ergibt sich also aus dem Informationsgehalt und der bestätigenden Handlung. Diese kann in jeder Form abgegeben werden; es empfiehlt sich aber eine (elektronische) schriftliche Form, da sie sich einfacher dokumentieren lässt.

Um die Kernkriterien einer datenschutzkonformen Einwilligung zu erfüllen, sollte eine datenschutzrechtliche Einwilligungsklausel nicht mit einer Lizenzvereinbarung (z. B. CC-Lizenz) gemischt werden. Anderenfalls ließen sich eine reine Nutzungslizenz und eine datenschutzrechtliche Einwilligung, die über die Lizenznutzung hinausgeht, nicht trennen. Der überstehende Teil wäre dann unfreiwillig erteilt worden, weil keine **„echte Wahlmöglichkeit"** bestand. Besagte datenschutzrechtliche Klausel sollte stets die einzelnen Zwecke aufschlüsseln (also **granular** sein) und auch zulassen, bei einer Vielzahl von Zwecken einzelne Zwecke abwählen zu können. Ist dies nicht der Fall, können begründete Zweifel an der Freiwilligkeit der Einwilligung auch zur Unwirksamkeit der Grundlage führen. Eine Orientierungshilfe bietet der Einwilligungs-Generator des ELDAH-Projektes.

Herausfordernd kann jedoch die Instabilität der Einwilligung sein, die sich aus dem Widerrufsrecht des Art. 7 Abs. 3 DSGVO ergibt. Danach kann eine Einwilligung jederzeit zurückgezogen werden, was die Grundlage für die weitere Verarbeitung unter die Kontrolle der betroffenen Person setzt und bei Entzug zugleich die Grundlage entzieht. Eine weitere Verarbeitung wäre deshalb unzulässig. Auf Bitte der betroffenen Person ist anschließend eine Löschung der Datensätze möglich (Art. 17 Abs. 1 lit. b). Dies umfasst auch jegliche Kopien, Replikationen, Links und Formen des Originaldatensatzes.

Zusatz zur Einwilligung: Wissenschaftliche Inhalte und Art. 85 DSGVO

Liegt ein wissenschaftlicher Kontext der Einwilligung wegen wissenschaftlicher Video-Inhalte vor, ergeben sich Abweichungen von den bisherigen allgemeinen Ausführungen. In Betracht kommt hier Art. 85 Abs. 1, 2 DSGVO, der die Möglichkeit für den Gesetzgeber eröffnet, abweichende Regelungen zugunsten wissenschaftlicher Kommunikationsinhalte vorzusehen. So dürfen die in einem Vortrag dargestellten Forschungsergebnisse nur dann personenbezogene Daten (beispielsweise auf den gezeigten Präsentationsfolien) enthalten,

wenn dies gem. § 27 Abs. 4 BDSG „für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist."

Für Vorträge relevanter ist jedoch das **Nebeneinander von Persönlichkeitsrecht und Datenschutzrecht**. Üblicherweise bedürfte es für die Einwilligung in eine Aufzeichnung und Veröffentlichung zweier Einwilligungen – eine gem. Art. 6 Abs. 1 lit. a, 7 DSGVO für das Datenschutzrecht, eine gem. §§ 22, 23 KUG für das Persönlichkeitsrecht. Denn: Das Datenschutzrecht bildet lediglich die Datenverarbeitung von der Erhebung (also Aufzeichnung) bis hin zur Veröffentlichung und anschließenden Verwertung ab – das Persönlichkeitsrecht in § 22 KUG aber nur das Recht am eigenen Bild und damit das Interesse an der Selbstdarstellung. Damit bildet letzteres nur das Ende eines Datenlebenszyklus ab. Außerdem erstreckt es sich zeitlich über den datenschutzrechtlichen Rahmen hinaus, indem es bei Ableben des/der Vortragenden einer Einwilligung eines:r Angehörigen bedarf.

Die Öffnung des Art. 85 Abs. 1, 2 DSGVO ermöglicht es aber, beide Einwilligungen gemeinsam zu erfassen; das Nebeneinander wird also für wissenschaftliche Kommunikationsinhalte (also auch Vorträge) gelockert. Für eine Einwilligung zur Veröffentlichung von Konferenzmitschnitten bedeutet dies, dass **ein einzelnes Einwilligungsdokument** ausreicht. Es sollte hierfür vollständig auf die Normenkette der Art. 6 Abs. 1 lit. a, 7 und 85 DSGVO in Verbindung mit §§ 22, 23 KUG verwiesen werden. Durch die Öffnungsklausel des Art. 85 DSGVO erstreckt sich das Verständnis des Einwilligungsbegriffes auch auf das KUG; obige Kriterien gehen also auf das Verständnis des KUG über und die Anforderungen gelten so auch hier.

Vertrag, Art. 6 Abs. 1 lit. b DSGVO

Ebenso denkbar ist eine Verarbeitung von Video-Aufzeichnungen auf Basis einer vertraglichen Übereinkunft der Beteiligten. Die Erhebung und Verarbeitung personenbezogener Daten in Form des Videos ist dann erforderlich „für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist". Denkbar wären hier Lehraufträge als wissenschaftliche Kommunikationsleistung (dann wissenschaftlicher Inhalt im Sinne des Art. 85 DSGVO, s. o.) oder beauftragte nicht-wissenschaftliche Erklärvideos zur Bedienung von Dienstleistungen (dann nicht-wissenschaftlicher Inhalt). Um den Vertragszweck für alle Beteiligten transparent und klar zu kommunizieren, sollte dieser unmissverständlich und konkret benannt werden. Dem widersprechen sehr offen und breit formulierte Verträge, die nicht mit den datenschutzrechtlichen Prinzipien der Transparenz und der Zweckbegrenzung vereinbar sind.

Die jeweiligen Verträge müssen aber zwischen der betroffenen Person und der veröffentlichenden Institution geschlossen werden. Ist noch eine vermittelnde Institution (z. B. eine die Konferenz organisierende Forschungsgesellschaft) beteiligt, so wird der Vertrag zwischen betroffener Person bzw. Vortragenden und dieser geschlossen. Die Plattform zur Speicherung und zum Abruf des Videos ist dann nur eine auftragsverarbeitende Stelle, die der Erfüllung des Vertrages – also der Veröffentlichung des Videos – dient. Wichtig ist in jedem Fall, dass die/der Vortragende **selbst beteiligt** und nicht nur mittelbar adressiert ist; ein Vertrag zwischen zwei Forschungsinstitutionen ist damit nicht von Art. 6 Abs. 1 lit. b DSGVO umfasst, da keine betroffenen Personen involviert sind.

Die Grenze des Zulässigen und des Vertragsinhaltes bildet hier das Kriterium der Erforderlichkeit. Bei der Aufzeichnung oder zur Nachbereitung erhobene, personenbezogene Daten müssen einen engen Bezug zum Vertragszweck haben. Es dürfen also nur die Datensätze verarbeitet werden, die für den Vertrag notwendig bzw. nicht wegzudenken sind. Beispielsweise ist es für die Veröffentlichung von Vorträgen und zur Förderung der Auffindbarkeit (also ein Teil der FAIR-Prinzipien) notwendig, dass der Name und ggf. die Forschungsinstitution benannt werden. Dadurch wird auch der Zusammenhang zwischen Vortragstitlel, -inhalten und der vortragenden Person hergestellt. Nicht erforderlich sind dagegen alle Informationen/Daten, die nicht der Vertragserfüllung – also der Veröffentlichung und Verbreitung des Vortrages – dienen; beispielsweise das Geburtsdatum, der Geburtsort und die Anschrift (außer im Falle einer Rechnung bei Honorar). Dies schließt auch Daten ein, die die Vertragserfüllung nur effizienter oder einfacher gestalten. **Erforderlichkeit meint hier also die Beschränkung auf das absolut Notwendige.**

Einen guten Überblick zur Gestaltung eines Vertrages bietet der Mustervertrag zur Datennutzung, der auf die einzelnen Abschnitte des Mustervertrages eingeht.

Berechtigtes Interesse, Art. 6 Abs. 1 lit. f DSGVO

Im Vergleich zu den übrigen Verarbeitungsgrundlagen ist das berechtigte Interesse des Art. 6 Abs. 1 lit. f DSGVO die weitreichendste Grundlage. Als berechtigt gilt **jedes wirtschaftliche, ideelle, wissenschaftliche oder geschäftliche Interesse**, sofern es tatsächlich besteht und nicht als Deckmantel für darunter liegende Zwecke genutzt wird. Dies ist jedoch nur dann der Fall, wenn die Interessen gegenüber den Interessen betroffener Personen (z. B. Redner:innen) überwiegen und die Datenverarbeitung für die Erfüllung/Erreichung der Interessen erforderlich ist. Damit wird der weite Zweck wieder begrenzt, wenn nicht jedes Datum, sondern nur die notwendigen Datensätze nutzbar sind. Es können sich folgende Fragen gestellt werden:

1. **Berechtigtes Interesse:** Welches Interesse habe ich an der Datenverarbeitung? Welchen Zweck möchte ich erfüllen?
2. **Erforderlichkeit/Datenumfang:** Ist die Datenverarbeitung wirklich zur Erfüllung meiner Ziele/Zwecke notwendig? Kann ich Teile oder den Zweck als solchen nicht auch durch andere Verarbeitungen erfüllen? Welche Daten brauche ich, um den beabsichtigten Zweck zu erreichen?
3. **Kein Überwiegen der Betroffeneninteressen:** Welche Interessen haben die Betroffenen, dass die Datenverarbeitung nicht durchgeführt wird – z. B. keine Kenntnis von der Verarbeitung, mangelhafte Schutzmaßnahmen, fehlende Anonymisierung/Pseudonymisierung/Verschlüsselung, etc.? Welche Maßnahmen kann ich dem entgegensetzen? Überwiegen meine Interessen die Betroffeneninteressen dann noch immer?

Außerdem ist zu erwähnen, dass diese im Ursprung einseitige Begründung der Datenverarbeitung einer **besonderen Information der Betroffenen** bedarf. Es reicht also nicht aus, frei verfügbare Datensätze zu sammeln und diese für die eigenen Zwecke (nach Prüfung obiger Schritte) zu nutzen. Sowohl bei einer Erhebung bei der betroffenen Person (Art. 13 Abs. 1 lit. d) als auch bei einer Erhebung über Dritte wie z. B. Soziale Netzwerke

(Art. 14 Abs. 2 lit. b) müssen die Interessen gegenüber der von der Erhebung betroffenen Person offengelegt werden.

Übertragen auf die Videoportal-Konstellation erscheint ein berechtigtes Interesse gegeben, wenn es um Datenverarbeitungen geht, die sich nicht vom Zweck der Ausrichtung einer Konferenz wegdenken lassen. Dies können beispielsweise statistische bzw. wissenschaftliche Erhebungen sein, die mit der Auswertung einer Konferenz (z. B. Evaluation) verbunden sind – insbesondere, wenn die Konferenz in ein Forschungsprojekt eingebunden ist. Dann bedarf es aber der Berücksichtigung besonderer Anforderungen an die wissenschaftliche Datenverarbeitung gem. Art. 89 DSGVO, § 27 BDSG und der allgemeinen datenschutzrechtlichen Prinzipien zur Datenminimierung und Speicherbegrenzung. Wirft man einen Blick auf die obigen Grundlagen, bleibt für eine Aufzeichnung und Verarbeitung (z. B. Upload) selbst kaum noch Raum. Eher könnte z. B. die Sicherheitskopie des Vortrags zu Archivierungszwecken ein berechtigtes Interesse darstellen. Besteht eine Rechtspflicht zur Archivierung, kommt dagegen Art. 6 Abs. 1 lit. c DSGVO ("Erfüllung einer rechtlichen Verpflichtung") in Betracht. Die wissenschaftlichen, nicht-gesetzlichen FAIR-Prinzipien können aber nicht als eine solche Rechtspflicht dienen (hierzu *Vettermann/Petri*, RuZ 1/2023).

Eine Besonderheit ergibt sich für das berechtigte Interesse daraus, dass es auch die berechtigte Interesse eines:r Dritten einbezieht. Die Konstellation aus Konferenzleitung als Mittlerin, Videoportal und Redner:in als betroffene Person findet sich also auch darin wieder. Beispielsweise könnte das Videoportal selbst zur Ausführung des Auftrags zwischen Videoportal – Konferenzleitung sich bei der Redner:in melden und die weiteren Schritte (Lizenz- und Datenschutzformulare abfragen; Aufzeichnung und Upload) eigenständig übernehmen. Das Video-Portal handelt dann im berechtigten Interesse der Konferenzleitung als "Dritter" im Sinne der DSGVO. Wichtig: Grundlage hierfür ist ein Auftragsverhältnis und eine klare Ausrichtung der Stellen zueinander. Das berechtigte Dritt-Interesse ergibt sich gerade erst aus dem Abhängigkeitsverhältnis. Bei einer datenschutzrechtlich gemeinsamen Verantwortlichkeit ist eher von "einem" (gebündelten) Verantwortlichen auszugehen; Änderungen im Prüfkatalog ergeben sich aber in beiden Fällen nicht, lediglich empfiehlt sich eine ausführlichere Dokumentation über die Informationsflüsse zugunsten eines vollständigen Verzeichnisses über Verarbeitungstätigkeiten (Art. 30 DSGVO).

Informationspflichten gem. Art. 13 und 14 DSGVO

Zu jeder Datenverarbeitung gehört eine Information der (betroffenen) Person, deren Daten verarbeitet werden. Zu unterscheiden ist stets dazwischen, ob die Daten bei der Person selbst (z. B. durch Eingaben der Person) oder über Dritte (z. B. die Konferenz-Leitung) erhoben werden. Eine **Informationspflicht ist damit stets gegeben**, jedoch existieren für jede Variante auch Ausnahmen.

Erhebung bei der Redner:in – Art. 13 DSGVO

Bei der Erhebung der Daten von/bei Redner:innen müssen folgende Informationen bereitgestellt werden; in der Darreichungsform ist die verarbeitende Stelle frei (z. B. Datenschutzerklärung):

- Name und Kontaktdaten der verantwortlichen Stelle, ggf. Vertretung
- wenn vorhanden: Kontaktdaten des/der Datenschutzbeauftragten ➞ Anforderungen: Art. 37 ff DSGVO
- Zweck(e) und Rechtsgrundlage(n) der Datenverarbeitung ➞ Art. 6, 9 DSGVO
- bei "berechtigtem Interesse": genaue Angabe dieser Interessen der verantwortlichen Stelle oder Dritter
- wenn vorhanden: Empfänger/Kategorien von Empfängern der personenbezogenen Daten
- wenn vorhanden: Absicht, Daten in ein Drittland (z. B. USA) zu übermitteln; eingeschlossen der Hinweis auf ein Vorliegen/Fehlen eines Angemessenheitsbeschlusses
- sofern geplant: Speicherdauer
- Hinweise auf Betroffenenrechte: Recht aus Auskunft; Recht auf Berichtigung/Löschung; Einschränkung der Verarbeitung; Widerspruchsrecht; Recht auf Datenübertragbarkeit (sog. Interoperabilität)
- nur bei Einwilligung als Rechtsgrundlage: Hinweis auf Widerrufbarkeit der Einwilligung (Ob und Wie)
- Hinweis auf Beschwerderecht bei (zuständiger) Aufsichtsbehörde
- bei gesetzlicher Verpflichtung als Rechtsgrundlage: Angabe der gesetzlichen Grundlage; auch Information über Konsequenzen einer Verweigerung der Weitergabe/Erhebung
- nur bei vollautomatisierter Verarbeitung (z. B. Entscheidungsfindung) gem. Art. 22 DSGVO: aussagekräftige Informationen über involvierte (technische) Logik und Tragweite der angestrebten Entscheidungen bzw. Verarbeitung für betroffene Person

Als einzige **Ausnahme** stellt Art. 13 Abs. 4 DSGVO von einer Information frei, wenn die betroffene Person bzw. Redner:in bereits über die Informationen verfügt.

Erhebung der Daten der Redner:in über Dritte – Art. 14 DSGVO

Werden die Daten nicht bei der betroffenen Person bzw. Redner:in erhoben, bedarf es einer ausführlichen Information. Schließlich rechnet die Person nicht mit der Erhebung, erlangt also erstmals Kenntnis von der Datenverarbeitung. Sie muss über folgende Informationen verfügen:

- Name und Kontaktdaten der verantwortlichen Stelle, ggf. Vertretung
- wenn vorhanden: Kontaktdaten des/der Datenschutzbeauftragten ➞ Anforderungen: Art. 37 ff DSGVO
- Zweck(e) und Rechtsgrundlage(n) der Datenverarbeitung ➞ Art. 6, 9 DSGVO
- bei "berechtigtem Interesse": genaue Angabe dieser Interessen der verantwortlichen Stelle oder Dritter
- wenn vorhanden: Empfänger/Kategorien von Empfängern der personenbezogenen Daten

- wenn vorhanden: Absicht, Daten in ein Drittland (z. B. USA) zu übermitteln; eingeschlossen der Hinweis auf ein Vorliegen/Fehlen eines Angemessenheitsbeschlusses
- sofern geplant: Speicherdauer
- Hinweise auf Betroffenenrechte: Recht aus Auskunft; Recht auf Berichtigung/Löschung; Einschränkung der Verarbeitung; Widerspruchsrecht; Recht auf Datenübertragbarkeit (sog. Interoperabilität)
- nur bei Einwilligung als Rechtsgrundlage: Hinweis auf Widerrufbarkeit der Einwilligung (Ob und Wie)
- Hinweis auf Beschwerderecht bei (zuständiger) Aufsichtsbehörde
- nur bei gesetzlicher Verpflichtung zur Verarbeitung: Angabe der gesetzlichen Grundlage; auch Information über Konsequenzen einer Verweigerung der Weitergabe/Erhebung
- nur bei vollautomatisierter Verarbeitung (z. B. Entscheidungsfindung) gem. Art. 22 DSGVO: aussagekräftige Informationen über involvierte (technische) Logik und Tragweite der angestrebten Entscheidungen bzw. Verarbeitung für betroffene Person

Aus der besonderen Situation – also dass die Daten über Dritte erhoben wurden – ergeben sich noch folgende Informationspflichten:

- aus welcher **Quelle** stammen die personenbezogenen Daten, insbesondere wenn diese **öffentlich** sind
- Frist zur Information: die Information ist so schnell wie möglich, **spätestens innerhalb eines Monats zu erteilen**
- werden dieselben Datensätze zur Kommunikation genutzt (z. B. E-Mail-Adressen): Information bereits in der ersten Mitteilung erfolgen
- sollen die Daten an weitere Empfänger/Dritte weitergegeben werden: Information muss spätestens zum Zeitpunkt der ersten Offenlegung gegenüber Dritten erfolgen

Ausnahmsweise kann eine Information in folgenden Fällen **entfallen**:

- die Redner:in verfügt bereits über obige Informationen;
- die Redner:innen können nicht erreicht werden, da unbekannt und/oder nicht ermittelbar (sog. Unmöglichkeit);
- die Kontaktaufnahme mit Redner:innen erfordert einen unverhältnismäßigen Aufwand (erfordert Abwägung);
- die Grundlage zur Erhebung der Daten sowie dazugehörige, geeignete Schutzmaßnahmen sind gesetzlich (national oder im Unionsrecht) geregelt ➞ in der Regel bei Verarbeitungsgrundlage gem. Art. 6 Abs. 1 lit. c oder e DSGVO;
- Teile der datenschutzrechtlichen Informationen (also der Liste oben) unterliegen nach nationalem oder Unionsrecht dem Berufsgeheimnisschutz.

———

Hinweis zum (subjektiven) unverhältnismäßigen Aufwand der Information von betroffenen Personen (z. B. Redner:innen): Diese Ausnahme ist gegeben, wenn öffentlich zugängliche Datensätze mit CC-Lizenzen frei verfügbar sind und entsprechende Vorträge gecrawlt (also automatisiert heruntergeladen, katalogisiert und annotiert) werden. Ganz gleich ob die Kontaktaufnahme unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist, sollte diese Feststellung inklusive Abwägung entsprechend dokumentiert werden. Zudem sind Verantwortliche mit dieser Ausnahme nicht vollständig aus der Informationspflicht entlassen, da dies den Zweck des Art. 14 DSGVO aushöhlen würde. Stattdessen sind "geeignete Maßnahmen zum Schutz [... der] betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit" zu treffen. Dies meint sowohl

- Vorkehrungen zur Berücksichtigung von Betroffenenrechten, z. B. Abfrage obiger Informationen im Detail (Auskunftsrecht) sowie einfacher Widerspruch gegen die Verarbeitung und Löschung der Datensätze,
- ggf. technische Schutzmaßnahmen zum Schutz der Datensätze (ohnehin nach Art. 25, 32 DSGVO zu treffen) und
- öffentlich abrufbare Information über datenschutzrechtliche Pflichten durch leicht zugängliche Information über obige Informationen, z. B. durch Meldungen in öffentlichen News-Portalen oder für alle Webseiten-Besucher:innen in einem nicht-abgegrenzten Bereich (z. B. ohne Login) ➞ “leicht zugänglich” meint dabei maximal 1-2 Klicks entfernt, z. B. als Addendum der Datenschutzerklärung.

Es reicht in Fällen öffentlich zugänglicher Datensätze wie Konferenzvideos nicht aus, von einer Einwilligung in Form der CC-Lizenz auszugehen oder die Information auf die ursprüngliche Veröffentlichungsplattform (z. B. YouTube oder Vimeo) abzuwälzen. Lizenzen aus dem Creative-Commons-Bereich sind per se nur für das Urheberrecht gedacht und dienen nicht als Einwilligung gegenüber der Allgemeinheit. Die DSGVO adressiert hier deutlich: Wer die Videos herunterlädt und verarbeitet wird (neuer) Verantwortlicher mit sämtlichen Rechten und Pflichten. Es bedarf also auch einer (eigenen) Rechtsgrundlage nach Art. 6 oder 9 DSGVO, die entsprechend öffentlich eingesehen werden kann. Dies muss in einem öffentlich für jede Person leicht zugänglichen Dokument (maximal zwei Klicks entfernt von der Startseite) eingesehen werden können. Eine Information auf Nachfrage ersetzt die Informationspflicht des Art. 14 DSGVO nicht, sondern ist letztlich nur die Erfüllung des Rechts auf Auskunft gem. Art. 15 DSGVO.

Automatisierte Verfahren und Besonderheiten des Art. 22 DSGVO

Je nachdem, ob und wie die Konferenzvideos aufbereitet werden sollen, können besondere Gründe für eine Verarbeitung in Betracht kommen. Werden beispielsweise vollständig automatisiert agierende Machine-Learning-Algorithmen zur Annotation und Analyse der Vortragsaufzeichnungen genutzt, könnte dies auf eine besondere Grundlage des Art. 22 Abs. 1, 2 DSGVO hinweisen. Dazu muss das Ergebnis des Algorithmus eine einzelfallbasierte Entscheidung darstellen. Die Einordnung ist vom Einzelfall abhängig, weshalb die Eckpunkte der Definition zur eigenen Einordnung skizziert werden.

Vorweg: **Artikel 22 DSGVO ist keine eigenständige Rechtsgrundlage.** Wie die übrigen Betroffenenrechte bietet Art. 22 Abs. 1 DSGVO die Möglichkeit, einer Verarbeitung – hier zu

Zwecken der automatisierten Entscheidungsfindung – zu widersprechen oder diese zu kontrollieren. Dafür muss es sich aber um eine (1) automatisierte Verarbeitung handeln, die zu einer (2) automatisierten Entscheidung (3) ohne menschliche Einwirkung führt und mit (4) einer rechtlichen Wirkung oder einer ähnlich erheblichen Beeinträchtigung verbunden ist.

1. **automatisierte Verarbeitung**: Es muss sich um eine Verarbeitung personenbezogener Daten handeln, die unter Nutzung technischer Mittel erfolgt. Damit verweist die Regelung auf den **Anwendungsbereich der DSGVO** (Art. 2 Abs. 1). Um dies für die eigenen Forschungsdaten zu überprüfen, empfiehlt sich der virtuelle Assistent von BERD@NFDI.
2. **automatisierte Entscheidung**: Der fragliche Algorithmus bzw. das fragliche Programm muss selbst ein Ergebnis zutage fördern, das auf der Verarbeitung der personenbezogenen Daten basiert. Die Art des Programms spielt dabei keine Rolle; das in der Regelung erwähnte "Profiling" ist nur exemplarisch zu verstehen. Auch kommt es nicht darauf an, wie komplex das Programm gestaltet ist. Prinzipiell ist daher jedes Programm hierunter zu verstehen, das eine oder mehrere Schlussfolgerungen als Ergebnis des Algorithmus trifft. Der Begriff ist also weit zu verstehen.
3. **ohne menschliche Einwirkung**: Auf den Prozess der (automatisierten) Entscheidungsfindung darf kein Mensch einwirken. Die Kette von der Einspeisung der personenbezogenen Daten bis zum Ergebnis (bzw. der Entscheidung) darf nicht durch menschliches Handeln unterbrochen werden. Beispielsweise unterbricht eine Überprüfung des Ergebnisses diese Kette, wenn das KI-Programm lediglich als Hilfsmittel zur Vorsortierung von Datensätzen dient. Der Mensch nimmt der KI dann die Entscheidung ab; es erfolgt keine rein algorithmische Entscheidung. Unter Umständen kann auch ein überwachtes Anlernen des KI-Systems hierunter zu verstehen sein. Wird die Kette jedoch nicht unterbrochen, kommt es zur Objektifizierung der betroffenen Person: Die betroffene Person (z. B. Redner:in) wird der rein technischen Entscheidung "unterworfen"; das Ergebnis wird einseitig vorgegeben und unterliegt nicht der Kontrolle der betroffenen Person.
4. **mit rechtlicher Wirkung/vergleichbare erhebliche Tragweite**: Dieses "Unterwerfen" muss aber mit einer entsprechenden Wirkung für die betroffene Person einhergehen. Eine rechtliche Wirkung ist gegeben, wenn an die Entscheidung unmittelbare Rechtsfolgen geknüpft sind – z. B. ein Vertrag (automatisiert) angenommen oder gekündigt wird. Rein mittelbare rechtliche Auswirkungen reichen nicht aus. Ähnlich belastend sind Entscheidungen, die die wirtschaftliche oder persönliche Entfaltungsfreiheit erheblich berühren, die körperliche Integrität/Gesundheit antasten oder die gesellschaftliche Reputation nachteilig verändern. Hier ist im Einzelfall zu prüfen, ob die (potentiellen) Ergebnisse der **Reputation von Wissenschaftler:innen**, – z. B. durch Bias der Trainingsdaten oder in der Programmierung – schaden können. Die Effekte können durch etwaige Schutzmaßnahmen abgemildert werden.

Sofern eine Situation gegeben ist, in der die Punkte 1 bis 4 gegeben sind, ist eine automatisierte Verarbeitung nur in folgenden **Konstellationen von Verarbeitungsgrundlagen** zulässig:

- Erfüllung eines **Vertrages** – Art. 22 Abs. 2 lit. a, 6 Abs. 1 lit. b DSGVO

- mitgliedsstaatliche **Rechtsvorschriften** – Art. 22 Abs. 2 lit. b, 6 Abs. 1 lit. c und/oder e und/oder 9 Abs. 2 lit. g DSGVO (beachte bei besonderen personenbezogenen Daten Art. 22 Abs. 4 DSGVO)
- (ausdrückliche) **Einwilligung** – Art. 22 Abs. 2 lit. c, 6 Abs. 1 lit. a und/oder 9 Abs. 2 lit. a DSGVO (beachte bei besonderen personenbezogenen Daten Art. 22 Abs. 4 DSGVO)

In anderen Fällen ist eine Verarbeitung rechtswidrig. Grund ist die Absicht der Regelung, Menschen nicht zum bloßen Objekt der Verarbeitung (sozusagen als Datenquelle) werden zu lassen. Ausgenommen ist damit u. a. das **berechtigte Interesse** einer verantwortlichen, verarbeitenden Stelle – allerdings nur, wenn es sich um eine obige automatisierte Entscheidungsfindung handelt. Mit Eingreifen eines Menschen ist Art. 22 Abs. 1 DSGVO nicht mehr erfüllt, weshalb automatisierte Assistenzsysteme (z. B. Web-Crawler) durchaus im Rahmen der Art. 6 Abs. 1, 9 Abs. 2 DSGVO zulässig sind. Die damit einhergehende Verarbeitung personenbezogener Daten löst allerdings eine Verantwortlichkeit aus, die zur Gewährung von Betroffenenrechten verpflichtet. Kurz: Jede Verarbeitung geht mit Verpflichtungen einher. Bei automatisierten Verarbeitungen mit Kenntnis der betroffenen Person (also bei Einwilligung und Vertrag) gem. Art. 22 Abs. 1 DSGVO werden die bereits aufgelisteten Betroffenenrechte durch folgende Rechte ergänzt bzw. modifiziert:

- **Recht auf Einwirkung/Eingreifen in den Entscheidungsprozess**: Durch die Einwirkung eines Menschen soll die rein automatisierte Verarbeitung aufgebrochen werden. Ziel ist eine Minimierung von Fehlern der Verarbeitung durch die menschliche Prüfungsinstanz. Hierfür genügt bereits eine allgemeine Plausibilitäts- und Richtigkeitskontrolle, außer es liegen nähere Informationen für eine Eingrenzung der Fehlerquelle vor.
- **Recht auf Darstellung des eigenen Standpunktes**: Durch die Darlegung der eigenen Sicht und ggf. tatsächlichen Sachlage soll ein Abgleich mit dem Entscheidungsergebnis ermöglicht werden. Dies schließt auch die Klarstellung von Informationen ein, die sich aus bzw. während des automatisierten Vorgangs ergeben. Damit stellt dieses Recht eine besondere Form des Rechts auf Berichtigung der eigenen Daten (Art. 16 DSGVO) dar. Aus diesem Recht können sich auch Indizien zum konkreten Eingreifen in den Prozess zur Fehlerbeseitigung ergeben.
- **Recht auf Anfechtung der Entscheidung**: Anfechtung meint hier nicht die Aufhebung der Entscheidung, sondern auch die inhaltliche Überprüfung und Fehlerkorrektur. Dies ist insbesondere dann der Fall, wenn sich die Anhaltspunkte aus einer Darstellung des eigenen Standpunktes verdichten und auf die Fehlerhaftigkeit der Entscheidung bzw. des Ergebnisses hinweisen.

Ein besonderer Fall liegt vor, wenn die **Verarbeitungskette aus einer oder mehreren automatisierten Verarbeitungsmechanismen** besteht. Dies ist zum Beispiel dann der Fall, wenn öffentlich verfügbare Vortragsvideos heruntergeladen und auf einer eigenen Plattform archiviert und im Anschluss auto-transkribiert, auto-verschlagwortet und auto-segmentiert werden. Auch wenn der gesamte Prozess als "eine Verarbeitung" gesehen werden könnte, empfiehlt es sich, derartige Schritte zur Begründung einer Verarbeitungsgrundlage aufzusplitten:

- **Web-Crawler**: Web-Crawler greifen in der Regel auf öffentlich zugängliche Datensätze zu. Daher ist zumindest bei besonderen personenbezogenen Daten (z. B. Gesundheitsdaten) von einem Bewusstsein über das Öffentlichmachen auszugehen (vgl. Art. 9 Abs. 2 lit. e DSGVO). Für "normale" personenbezogene Daten fehlt diese Ausnahme. Hier kann sich lediglich auf das berechtigte Interesse des Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Denn: Im Rahmen der Abwägung kann die Öffentlichkeit der Datensätze eingebracht werden als Argument, dass die betroffene Person scheinbar kein Interesse am weiteren Verbleib der Daten hat. Öffentlich gemachte Datensätze sind "verloren". Doch Vorsicht: Es kann sich stets auch um **Daten** handeln, **die die Person nicht selbst öffentlich gemacht hat**. **Hier ist sorgfältig und im Einzelfall zu prüfen, ob dies der Fall ist.** Voraussetzung für eine Verarbeitung ist auch, dass sich nur auf die für den Verarbeitungszweck notwendigen Daten beschränkt wird. Denn auch die Verarbeitung öffentlich zugänglicher personenbezogener Daten ist eine Verarbeitung personenbezogener Daten, die mit entsprechenden Verantwortlichkeiten einhergeht.
- **Auto-Segmentierung**: Auch die automatische Segmentierung mittels Analyse der Bild- und Ton-Daten stellt eine Verarbeitung personenbezogener Daten dar. Andernfalls wäre im Einzelfall nachzuweisen, dass sich die Segmentierung nur auf den Bildteil beschränkt, in dem die betroffene Person nicht zu sehen ist. Da es aber in der Regel gerade für diese Unterscheidung der automatisierten Erkennung der bzw. einer Person bedarf, ist von einer relevanten Verarbeitung auszugehen. Auch eine Auto-Segmentierung lässt sich mit dem berechtigten Interesse des Art. 6 Abs. 1 lit. f DSGVO vereinbaren bzw. begründen. Hier spielen dann zugunsten der verantwortlichen Stelle vor allem die **FAIR-Prinzipien** eine Rolle, um das Video zugänglicher und zitierbarer zu gestalten. Selbst wenn die automatisierte Entscheidung in Form der Setzung der Kapitelmarke eine Entscheidung gem. Art. 22 Abs. 1 DSGVO darstellt, so ist sie für die betroffene Person nicht erheblich genug. **In der Regel stellt diese Verarbeitung kein Problem dar.**
- **Auto-Transkription**: Eine Auto-Transkription – also die automatisierte Übersetzung von Ton- bzw. Sprachdaten in Texte zur Zugänglichmachung der Vortragsinhalte – stellt eine automatisierte Verarbeitung personenbezogener Daten dar. Problematisch ist dabei, dass die Übersetzung mittels Maschinellem Lernen (nachfolgend ML) generierten Wortschatz sich erheblich auf das Merkmal der erheblichen Wirkung der automatisierten Entscheidung (also des Übersetzungstextes) auswirkt: Je nach Basiswortschatz übertragen sich Bias bzw. Verzerrungen in dem ML-Datensatz und damit aus den Trainingsdaten in die Übersetzung des Vortrags selbst. Ein Beispiel: Ein ML-Algorithmus wird so trainiert, dass er Vorträge zur Philosophie einwandfrei übersetzt. Wird ein Video einer Mathematik-Vorlesung diesem ML-Algorithmus vorgelegt, kann sich daraus nicht nur eine mangelhafte Übersetzungsleistung ergeben. Die fehlerhafte Übersetzung kann – je nach ML-Trainingsdatensatz – auch falsche Forschungsaussagen generieren, die dank einer Auto-Segmentierung auch so zitierbar sind. Damit unterstellt die automatisierte Transkription Forschungsaussagen der Forscher:in, die so nie geäußert wurden. Gerade im kulturhistorischen oder geisteswissenschaftlichen Kontext, das von einem **ethischen Bewusstsein im Diskurs über kulturhistorische Forschungsdaten** geprägt ist, ist dies der Reputation der Forscher:in eher schädlich. Ein unüberwachter ML-Algorithmus mit entsprechenden Bias birgt die Gefahr unethischer Aussagen, die sich nachteilig auf

die Reputation und damit auf die Forschungsfreiheit der betroffenen Redner:in oder sogar auf die Institution als solche auswirken. Eine Google-Indizierung der Webseite sowie Snapshots auf Web-Archiven tragen dazu bei, dass die Reputation auch nachhaltig beeinträchtigt werden kann. Die Argumente der Erheblichkeit der automatisierten Entscheidungen sind damit gegeben, dass eine Auto-Transkription nur im Rahmen des Art. 22 Abs. 1 DSGVO – also nach Einwilligung der Redner:in sowie eigenhändiger Prüfung des Textes oder auf Basis eines Lizenzvertrages ebenso inklusive Prüfungsmöglichkeit – zulässig ist. Eine Verarbeitung allein auf Basis eines berechtigten Interesses gem. Art. 6 Abs. 1 lit. f DSGVO ist unzulässig, da das Interesse hier nicht überwiegen kann: Die betroffene Redner:in hat ein stetiges Interesse an der Richtigkeit der Information, also besagte Übersetzungen gegenzuprüfen. Hier können auch die **FAIR-Prinzipien** als nicht-rechtliche, rein wissenschaftliche Grundsätze nicht entlastend wirken, da sie aufgrund ihres Charakters die Forschungsfreiheit und Reputation nicht einschränken können bzw. sollen (siehe DFG-Positionspapier zu Open Science, S. 7 ff.). **Im Zweifel ist also von einer Auto-Transkription abzusehen und diese nicht standardmäßig und nur nach unmittelbarer Rücksprache mit der Redner:in bzw. Forscher:in vorzunehmen.**

- **Auto-Verschlagwortung**: Auch eine Auto-Verschlagwortung stellt kann eine Verarbeitung personenbezogener Daten darstellen. Ergibt sich die Verschlagwortung beispielsweise **aus den Abstract-Texten zu den Vorträgen**, enthalten diese oftmals kurze Informationen über die Wissenschaftler:in (Name, Position, Affiliation, Kontaktdaten, etc.). **Dies stellt in der Regel kein Problem dar**, da dies ganz nach der Argumentation zum Web-Crawling dem berechtigten Interesse (Art. 6 Abs. 1 lit. f DSGVO) dient und so die gecrawlten Vortragsvideos erst zugänglich und auffindbar gemacht werden. Die Argumentation der Abwägung ist damit wieder durch die FAIR-Prinzipien dominiert. Ob und inwieweit Betroffeneninteresse überwiegen, ist im Einzelfall zu prüfen. Bei dem eigens verfassten und öffentlich gemachten Abstract werden regelmäßig die besseren Argumente für ein Interesse der verantwortlichen Stelle sprechen, die Gewährleistung der Betroffenenrechte vorausgesetzt. **Basiert die Auto-Verschlagwortung dagegen auf der Auto-Transkription**, vererben sich die Fehler der mangelhaften Transkription auf die Verschlagwortung: Es besteht auch hier das Risiko, dass Falschanalysen zu einer Verschlagwortung mit inhaltlich falschen oder gar unethischen Begriffen führen. Auch diese Übertragen sich auf die Indizierung in Suchmaschinen, gegen die sich aus Betroffenensicht nur mäßig gewehrt werden kann. Eine zulässige Grundlage wäre auch hier nur durch Art. 22 Abs. 1 DSGVO in Verbindung mit dem jeweiligen Verarbeitungsgrund des Art. 6 Abs. 1 DSGVO – also nach Einwilligung der Redner:in sowie eigenhändiger Prüfung der Schlagworte oder auf Basis eines Lizenzvertrages ebenso inklusive Prüfungsmöglichkeit – zulässig. Das berechtigte Interesse des Art. 6 Abs. 1 lit. f DSGVO kann auf Basis der FAIR-Prinzipien nicht überwiegen, da die mangelhafte Verschlagwortung die Auffindbarkeit und Zugänglichkeit der Aufzeichnungen eher beeinträchtigt als fördert. **Eine Auto-Verschlagwortung sollte deshalb nicht auf einer Auto-Transkription basieren.**

Hinweise zu Videoportalen außerhalb der EU – Art. 44 ff DSGVO

Auch für die Übermittlung der Videoaufzeichnungen an Videoportale (kurz: Upload) sind die verantwortlichen Stellen (z. B. aufzeichnende Person/Institution) verantwortlich und müssen das europäische Datenschutzniveau der DSGVO gewährleisten. Verlässt der Datensatz die EU – z. B. um das Video auf öffentlich zugänglichen Servern zu speichern – und wird in ein Drittland übertragen, müssen die Betroffenenrechte und die Grundsätze der DSGVO weiterhin gewahrt werden. Drittland meint dabei jeden Staat, der nicht EU-Mitgliedsstaat ist. Die EWR-Staaten Island, Liechtenstein und Norwegen bilden hier die Ausnahme und sind wie EU-Staaten zu behandeln, da sie äquivalente Datenschutz-Regelungen getroffen haben. Bei Auswahl des Dienstleisters und/oder den Einstellungen im Hintergrund hat die verantwortliche Stelle also entsprechende Sorgfalt walten zu lassen.

Finden dadurch Verarbeitungen in einem Drittland statt, muss die verantwortliche Stelle die Regelungen der Art. 44 ff DSGVO erfüllen und den Datenschutz gewährleisten. Dabei gibt die DSGVO stufenweise folgende Instrumente vor, die 1. Stufe wäre also der 3. Stufe vorzuziehen:

1. **Angemessenheitsbeschluss der Europäischen Kommission**: Handelt es sich um ein (datenschutzrechtlich) sicheres Drittland, hat die Europäische Kommission einen Angemessenheitsbeschluss erlassen. Damit besteht im Drittland ein angemessenes Datenschutzniveau, das dem der DSGVO entspricht. Es bedarf also keiner besonderen Maßnahme, um die Betroffenenrechte und Grundsätze der DSGVO zu bewahren. Stattdessen kann auf die gewohnten, auch im EU-Raum genutzten Mittel und Wege zurückgegriffen werden.
2. **Standarddatenschutzklauseln**: Werden die Daten in ein (datenschutzrechtlich) unsicheres Drittland übertragen, kann von den Beteiligten auf sog. Standarddatenschutzklauseln zurückgegriffen werden. Dabei handelt es sich um von der EU vorgegebene Klauseln, die in den Vertrag (ähnlich wie AGB) unverändert einbezogen werden. Sie enthalten regelmäßig Regelungen, die Betroffenenrechte und -interessen besonders schützen. Eine Abänderung zu Lasten der Betroffenen ist daher unmöglich; eine positive Ergänzung mit strengeren Regelungen zur Gewährleistung/Erhöhung des Schutzniveaus dagegen zulässig. Ein Aufheben der Klausel-Beschlüsse ist nur durch den Europäischen Gerichtshof (EuGH) möglich. Welche Standarddatenschutzklauseln zu wählen sind, hängt vom Einzelfall ab. Die EU hat im jüngsten Beschluss (Stand: 20.2.2023) ein modulares System geschaffen. Darin werden alle Situationen zwischen mehreren verantwortlichen und auftragsverarbeitenden Stellen erläutert.
    - Für Videoportale werden mit Blick auf die obigen Konstellationen wohl entweder das Modul 1 (Verantwortlicher–Verantwortlicher) und/oder das Modul 2 (Verantwortlicher–Auftragsverarbeiter) benötigt.
    - Eine wichtige Anmerkung ergibt sich aus dem EuGH-Urteil Schrems II: Eine Einbindung von Standardvertragsklauseln allein reicht nicht aus, um ein mangelhaftes Datenschutzniveau auszugleichen. Je nach beteiligtem Land sind gesonderte, ergänzende Maßnahmen zu treffen. Das ist insbesondere dann der Fall, wenn die Verarbeitung in einem Land geschieht, in dem der Zugriff von Behörden auf unternehmerische Datensätze ungehindert möglich

ist und nicht durch Schutzmaßnahmen verhindert werden kann. Im Urteil wurde dies für die USA festgestellt. Dort ist der NSA der Zugang zu den Telekommunikationsdaten des Dienstleisters Cloudflare von Gesetzes wegen möglich. Ähnliches lassen Medienberichte zu Anfragen der US-Sicherheitsbehörden bei Google und Apple vermuten. In der Regel ist damit anzunehmen, dass eine Verarbeitung in den USA auch nicht bei Vorliegen von Standarddatenschutzklauseln zulässig ist. **Dienste mit einem Server-Standort oder zumindest Impressum/Sitz in den USA sind damit zu meiden, sofern die Datenschutzerklärung den Speicherort nicht explizit in der EU angibt.**

3. **Ausnahmeregelung des Art. 49 DSGVO**: Sind sowohl Angemessenheitsbeschluss als auch Standarddatenschutzklauseln nicht gegeben, handelt es sich um ein (datenschutzrechtlich) unsicheres Drittland. Erst dann kommen die Ausnahmetatbestände des Art. 49 DSGVO zur Anwendung. Dies geht jedoch stets mit dem Risiko einher, dass die personenbezogenen Daten der Betroffenen gar nicht oder nicht mehr effektiv geschützt sind. Die Regelungen sind daher mit großer Vorsicht zu nutzen. **In jedem der nachstehenden Ausnahmefälle verzichtet die betroffene Person auf den Datenschutz. Damit verabschiedet sie sich letztlich vom grundrechtlich gewährleisteten Schutz.** Relevant sind vor allem folgende Ausnahmen:

    - **Ausdrückliche und besonders informierte Einwilligung, Abs. 1 lit. a**: Willigt die betroffene Person in die Weitergabe der Daten ein, muss sie über die Risiken der Aufgabe der Kontrolle über die eigenen Daten (z. B. über die Betroffenenrechte) ausdrücklich hingewiesen werden. Es ist zu benennen, in welche Länder die Datenübertragung erfolgt, dass in diesem Drittland kein gleichwertiges Datenschutzniveau existiert, gegebenenfalls staatliche Stellen ungehindert auf die Datensätze zugreifen können (siehe EuGH-Urteil Schrems II – Zusammenfassung des BfDI) und welche Konsequenzen die Weitergabe perspektivisch haben kann. Sollten nur einzelne Betroffenenrechte durchsetzbar sein, sind diese gesondert zu benennen. Dies gilt auch, wenn diese nur teilweise erfüllt werden können. Erst dann tritt ein ausreichendes Informiertsein ein, um eine wirksame Einwilligung abgeben zu können.

    - **Vertragserfüllung, Abs. 1 lit. b und c**: Im Kern greift die DSGVO hier die Verarbeitungsgrundlage des Art. 6 Abs. 1 lit. b DSGVO auf. Umfasst sind auch vorvertragliche Maßnahmen oder notwendige Nebenpflichten. Die Ausnahme ist jedoch nicht weit zu verstehen, im Gegenteil: Eine Übermittlung personenbezogener Daten ist nur vorzunehmen, wenn dies für das Vertragsziel nicht anders zu bewerkstelligen und damit unvermeidbar ist. Beispielsweise kann für die Buchung eines Flugtickets oder Hotelzimmers in einem Drittland kaum eine Datenverarbeitung zur Vertragserfüllung (Reisevertrag; Unterbringungsleistung) vermieden werden. Anders liegt die Sache, wenn sich zur Abrechnung der Vortragshonorare eines nicht-europäischen Dienstleisters bedient wird, obwohl es gleichwertige europäische/deutsche Dienstleister gibt – hier darf nicht zugunsten der Wirtschaftlichkeit und Sparsamkeit das günstigere, aber rechtlich risikoreichere Angebot gewählt werden. Handelt es sich dagegen um eine

Vertragserfüllung, die im Interesse der betroffenen Person liegt (Art. 49 Abs. 1 lit. c), muss die Eindeutigkeit des Interesses dokumentiert und ggf. nachgewiesen werden können. Auch hier bedarf es eines engen und erheblichen Zusammenhangs zwischen Vertragsleistung und Datenübertragung. Sie muss unvermeidbar sein, um den Vertrag zu erfüllen.

- **Öffentliches Interesse, Abs. 1 lit. d**: Öffentliche Interessen meint hier ausschließlich Interessen, die im Unionsrecht oder Recht des Mitgliedsstaates verankert sind. Nicht gemeint sind damit mit öffentlichen Geldern geförderte Forschungsprojekte, wenngleich diese mit einem öffentlichen Interesse der Allgemeinheit in Verbindung stehen. "Öffentlich" meint hier eher "öffentlich-rechtlich" oder "staatlich".
- **Wahrung zwingender berechtigter Interessen**: Im Kern greift die DSGVO hier auf das berechtigte Interesse des Art. 6 Abs. 1 lit. f DSGVO auf. Sofern sich auf diese Verarbeitungsgrundlage berufen wird, ist aber nicht zugleich **Art. 49 Abs. 1 UAbs. 2 DSGVO** erfüllt. Vielmehr bedarf es weiterer Voraussetzungen, die die Begründung der Datenübermittlung stark einschränken. So darf es sich nur um eine einmalige Übermittlung handeln, die nur eine begrenzte Anzahl von betroffenen Personen betrifft, zur Wahrung berechtigter Interessen erforderlich ist und die Interessen betroffener Personen nicht überwiegen. Zudem müssen bestmögliche Maßnahmen getroffen werden, um den (verbleibenden) Schutz des Datenschutzniveaus zu erhalten. Wahl und Ausgangslage muss die verantwortliche Stelle dokumentieren. Vor der Übermittlung ist die zuständige Aufsichtsbehörde in Kenntnis zu setzen; die betroffene Person ist ebenfalls nach den Informationspflichten der Art. 13 oder 14 DSGVO zu informieren. Kurzum: **Eine zulässige Übermittlung auf dieser Grundlage erscheint höchst unwahrscheinlich; hiervon ist abzuraten.**

Abschließend ist der Upload von Vortragsaufzeichnungen in diese Ausführungen einzuordnen: Ein **Upload bei gängigen Video-Portalen wie YouTube oder Vimeo** geht stets mit einer Übermittlung an amerikanische Server-Zentren einher. YouTube hat seinen Firmensitz in Irland bzw. Mountain View (Californien), Vimeo in New York (USA). Auch wenn der Firmensitz nicht notwendigerweise mit dem Standort der Server übereinstimmen muss, wirkt das Impressum zumindest als Indiz. Im Einzelnen geben die Datenschutzerklärungen auch Aufschluss über die Datenübermittlung. Damit bewegt sich die Datenverarbeitung stets im Bereich der Schrems-II-Rechtsprechung des EuGH. Nutzungsvereinbarungen, z. B. im Rahmen der Kanal-Eröffnung auf YouTube, reichen bei einer Einbeziehung (auch aktueller) Standarddatenschutzklauseln nicht aus. Es bedarf zusätzlicher Schutzmaßnahmen, um das europäische Datenschutzniveau zu gewährleisten. Dies ist für Forschungsinstitute aber unmöglich. Somit kommen ausschließlich die Ausnahmen in Betracht, insbesondere die Einwilligung des Art. 49 Abs. 1 lit. a DSGVO. Hier muss aber unbedingt die gesonderte, ausführliche Informationspflicht erfüllt werden. Ein bloßes "Wir veröffentlichen Ihr Video auf YouTube. Damit können wir den Datenschutz nicht mehr garantieren." reicht nicht aus. Für Nutzer:innen und Vortragende als Nicht-Jurist:innen ist nicht nachvollziehbar, was diese "fehlende Garantie" bedeutet. Es gelten hier also strenge Grundsätze der Transparenz und der "klaren und einfachen Sprache", die schon für die gewöhnliche Einwilligung nach Art. 6 Abs. 1 lit. a, 7 DSGVO gelten. **Damit ist auch die Nutzung dieser Ausnahme ausdrücklich**

nicht empfohlen, da bei häufigem/regelmäßigen Gebrauch von einer Umgehung des Datenschutzrechts der Forschenden ausgegangen werden könnte.

———

Datenschutzerklärung für nicht-wissenschaftliche Inhalte

Vorab: Nicht-wissenschaftliche Inhalte

Nicht-wissenschaftliche Inhalte meint die Verbreitung von Informationen mit geringem bzw. losem Wissenschaftsbezug. Es fehlt also an einem Zusammenhang zwischen dem Forschungsprozess und der Darstellung in Videoform. Beispielsweise sind dies Informationsvideos über die Anwendung von Annotationsprogrammen für die Wissenschaftscommunity als Dienstleistungen („How to“) oder ein Einführungsvideo über die Nationale Forschungsdateninfrastruktur. Es reicht nicht aus, dass die Person selbst eine akademische Laufbahn hat bzw. einen Titel trägt oder das Konsortium überwiegend aus wissenschaftlichen Partnern/Institutionen besteht.

Allgemeine Anforderungen

Für nicht-wissenschaftliche Inhalte ergeben sich keine spezifischen Besonderheiten. Der lose Wissenschaftsbezug führt in der Regel dazu, dass es zu keiner Darstellung von Forschungsdaten – und somit personenbezogener Daten Dritter – kommt. Vielmehr sind in Informationsvideos höchstens die Stimme und ggf. Name und Affiliation der Redner:in zu sehen. Damit gelten die üblichen datenschutzrechtlichen Grundsätze, die bereits für wissenschaftliche Inhalte dargestellt wurden. Für Verarbeitungsgrundlagen, die Gewährleistung von Betroffenenrechten, automatisierte Verarbeitungen oder den Upload von Informationsvideos auf Video-Portalen in Drittländern gelten damit die gleichen Grundsätze. Dies ist jedoch ggf. je nach Einzelfall anders zu bewerten.

Zur Einwilligung: Nicht-wissenschaftliche Inhalte und §§ 22, 23 KUG

Eine wichtige Änderung ergibt sich mit Blick auf Konferenzinhalte oder sonstige Videoformate ohne wissenschaftlichen Inhalt. Hier bleibt das bereits zuvor skizzierte parallele Verhältnis von Datenschutzrecht (DSGVO, BDSG) und Persönlichkeitsrecht (KUG) bestehen. Damit bedarf es der **Abfrage zweier einzelner Einwilligungen**, die zwar in einem einzelnen Dokument stehen können. Die Granularität, also die jeweilig abgegrenzte Einwilligung, ist jedoch für bestimmte Anwendungsfälle in der Praxis durchaus denkbar: So ist eine datenschutzrechtliche Einwilligung schon für die Anfertigung der Videoaufzeichnung relevant; die Einwilligung nach KUG erfasst dies nicht. Wünscht der/die Vortragende nur eine Aufzeichnungen für private Zwecke (z. B. als Andenken), müsste er/sie in die Aufzeichnung nach DSGVO einwilligen, aber die Veröffentlichung nach KUG ablehnen können. Auf diese Weise bleibt die Freiwilligkeit bei beiden Einwilligungen erhalten und der/die Forscher:in kann eigenständig entscheiden, wie er/sie sich in der Öffentlichkeit mit welchen Inhalten präsentieren möchte.