Mustervertrag
Datennutzung KonsortSWD:
Erläuterungen und rechtliche Fragen

Version 1.0.0., Stand: 20.01.2022

Inhalt

Vorbemerkung und Erläuterung zum „Mustervertrag Datennutzung KonsortSWD Version 1.0.0“

Dieser Musterdatennutzungsvertrag wurde 2021 im Auftrag von und in Zusammenarbeit mit dem Konsortium für die Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften (KonsortSWD) erarbeitet.
Basis waren Datennutzungsverträge von Forschungsdatenzentren (FDZ), die durch den RatSWD akkreditiert sind. Auf freiwilliger Basis stellten 20 FDZ ihre Datennutzungsverträge für die Konzeption eines harmonisierten Vertrags zur Verfügung. Darauf aufbauend wurde unter Hinzuziehung der Kanzlei iRights.Law Rechtsanwälte ein Vertrag für die Datenbereitstellung und -nutzung – insbesondere auch personenbezogener Daten – im In- und Ausland unter Berücksichtigung der DSGVO erarbeitet.
Die nachfolgenden Hinweise dienen der Erläuterung der einzelnen Abschnitte des Vertrages. Im Anschluss finden sich außerdem einige allgemeine Fragen, die im Vorfeld der Vertragserstellung aufgetaucht sind, die hier (allerdings nur) kursorisch beantwortet sind.

Fakultative Elemente sind in diesem Mustervertrag durch ein Kästchen gekennzeichnet (❑).
In Fällen in denen eine von mehreren Alternativen ausgewählt werden muss, ist dies durch Kreise gekennzeichnet (❍). In der Bearbeitung eines Vertrages können die jeweiligen Elemente entweder durch ein „x“ markiert werden, oder die unzutreffenden gestrichen werden.

Diese erste Fassung eines Mustervertrages für wissenschaftliche Datennutzung ist sicherlich noch nicht als der Weisheit letzter Schluss zu lesen; Praxistaugliche und institutionsübergreifende Vertragsmuster erfordern in der Regel weiteren Diskurs unter den Institutionen - nur so kann ein gemeinsamer Standard entstehen. Hierfür stellt das vorgelegte Dokument einen geeigneten Ausgangspunkt dar. Es ist davon auszugehen, dass sich einige der (Fakultativ-)klauseln in der Praxis als kaum relevant erweisen, welche daher in zukünftigen Fassungen gestrichen werden können. Gleichzeitig ist nicht auszuschließen, dass Bedarf für weitere Klauseln/Regelungsaspekte bestehen kann, die auch in eine zukünftige Version einfließen können.

Erläuterungen zur Bestimmung der Vertragsparteien

Die Bestimmung der Parteien in einem Datennutzungsvertrag unter Beteiligung eines Forschungsdatenzentrums stellt regelmäßig ein sog. Mehr-Personen-Verhältnis dar, in dem Rechte und Pflichten zwischen der Datengebenden Stelle, dem FDZ und den Datennutzenden geregelt werden.
Dabei können bei den Datennutzenden wiederum auch Pflichten untereinander begründet werden. Sofern mehrere Datennutzende die Daten in eigener Verantwortlichkeit verwenden und gleichzeitig der Austausch über die Daten ermöglicht werden sollen, besteht zudem für die Datennutzenden untereinander ein Verhältnis gemeinsamer Verantwortlichkeit nach Art. 26 DSGVO.
Insgesamt deckt der Mustervertrag eine Vielzahl von Fallkonstellationen ab. Das Spektrum reicht von Vereinbarungen mit Forschungskonsortien über solche mit Lehrenden, die die Daten etwa im Rahmen eines Seminars ihren Studierenden zur Verfügung stellen, bis hin zu einfachen Konstellationen in denen der (hauptverantwortlich) Datennutzende ein/e einzelne/r Forscher/in ist und keine weiteren Datennutzenden einbezogen werden. In Konstellationen, in denen mehrere Datennutzende berechtigt werden sollen, ist hier nur der oder die Hauptverantwortliche zu nennen, alle weiteren sind über den entsprechenden Anhang in den Vertrag einzubeziehen.
Datennutzende, verantwortliche Stellen können jur. Personen („Institutionen“) sein, die dann durch eine natürliche Person vertreten werden. Diese vertretungsbefugte Person muss nicht der Person entsprechen, die dann tatsächlich mit den Daten arbeitet. Letztere sollte dann als „einfacher“ Datennutzender über den Anhang aufgenommen werden. Alternativ kann auch eine natürliche Person Hauptverantwortlich Datennutzende/r sein. In diesem Fall kann die Nutzungsbefugnis an die Zugehörigkeit zu einer Institution gekoppelt werden.
Weitere Datennutzende sollten ebenfalls im Anhang „Datennutzende“ genannt sein oder später über den Anhang „Vertragserweiterung: Datennutzende“ hinzugefügt werden.

Ein FDZ wird hingegen stets eine Institution sein, weswegen hierbei stets ein (oder mehrere) Vertretungsbefugte(r) anzugeben sind.
Bei den Datengebenden kann es sich allerdings auch wieder um natürliche oder juristische Personen handeln. Ebenfalls ist denkbar, dass das FDZ selber auch datengebende Stelle ist, entweder, weil die Daten aus dem eigenen Bestand kommen oder dieser von den Primärforschenden in die Verantwortlichkeit des FDZ überantwortet wurde.

Erläuterung zu § 1 Hauptpflichten

Die Hauptpflichten bedürfen vermutlich keiner umfangreichen Erläuterung. Sie sollten den Erwartungen der Parteien entsprechen.

Erläuterung zu b) Zugänglichmachung der Datenbasis

Der genaue Zugangsweg unterscheidet sich je nach FDZ und auch innerhalb der FDZ werden unterschiedliche Zugänge mit jeweils eigenen Bedingungen angeboten; entsprechend sind die hierfür relevanten Regelungen in einen getrennten Anhang ausgelagert.

Erläuterung zu c) Verantwortliche Datenverarbeitung

Die besondere Verantwortung der Datennutzenden wurde hier noch einmal unterstrichen, hätte aber auch in eine Präambel Eingang finden können. Die Klausel enthält darüber hinaus eine Abwägungsklausel zugunsten der Betroffenen, die insoweit in Grenzfällen eine Erleichterung der Rechtsfindung ermöglichen soll.

Erläuterung zu d) Entgelt gemäß Kostenmodell

Etwaige Kostenregelungen sind einrichtungsspezifisch und lassen sich nach derzeitigem Stand nicht vereinheitlichen. Daher sollten sie in einem getrennten Anhang geregelt werden. Dort können ggf. Regelungen zur Anpassung der Gebühren integriert werden, so auch ein etwaiges Sonderkündigungsrecht bei Anhebungen der Gebühren im laufenden Vertragsverhältnis.

Erläuterung zu § 2 Verarbeitungszweck

Die Regelungen zum Verarbeitungszweck sind elementar für die Reichweite des Nutzungsrechts und dienen gleichzeitig als datenschutzrechtlich erforderliche Zweckbeschränkung.
Das Muster sieht zwei Generalklauseln jew. eine Wissenschaft und eine für Lehre vor. In der Regel wird aber auch aufgrund der geforderten Zweckspezifizität zu empfehlen sein, das Vorhaben in einem getrennten Anhang (kurz) zu beschreiben. Über diese Variante können auch Vorhaben dargestellt werden, die sowohl Forschung als auch Lehre vereinen.

Erläuterung zu § 3 Nutzungsdauer

Die Regelungen zur Nutzungsdauer bilden die verschiedenen Ansätze der Praxis ab. Es besteht die Option zur unbefristeten Nutzungsrechteinräumung, zur Befristung auf einen Zeitraum oder eine Anknüpfung an ein beschriebenes Vorhaben. Darüber hinaus sind verschiedene Kündigungsregelungen vorgesehen. Außerdem besteht die Möglichkeit der Kündigung aus wichtigem Grund, die sich bereits aus gesetzlichen Vorgaben ergibt und im Abschnitt Vertragsverstöße erwähnt wird.
Insbesondere die Regelung der einseitigen, unbegründeten Kündigung durch die Datengebende Stelle dürfte für Datennutzende zumeist nur schwer hinnehmbar sein. Sie wurde aber aufgenommen, weil sie in mehreren Verträgen so oder in ähnlicher Form wieder zu finden war und daher vermutet wird, dass einzelne Datengebende Stellen auf diesem Vorbehalt bestehen.
Umgekehrt erscheint ein ordentliches Kündigungsrecht für die Datennutzenden unproblematisch; allerdings ist dieser Fall im Rahmen einer Entgeltregelung (im entsprechenden Anhang) zu

berücksichtigen. Die Beschränkung des Zugangs könnte auch im Rahmen der TOMs vereinbart werden, trifft aber das FDZ und passt daher systematisch besser hier.
Vielfach wird die Vertragslaufzeit auch an die Zugehörigkeit zu einer Institution geknüpft – vermutlich weil diese einen Vertrauensanker für die Einhaltung des Vertrages darstellt. Daher ist dies als Option vorgesehen. Ob ein Institutionswechsel automatisch zu einer Kündigung führen muss, hängt davon ab, wie das jeweilige Vorhaben personell strukturiert ist. Die Bindung einzelner Beteiligter an eine Institution kann über den Anhang Datennutzende deutlich gemacht werden, so dass die Anwendung dieser Klausel auf diese Beteiligten beschränkt werden kann.
Die Mitteilungsregelungen zu Anhang Datennutzende könnten sicherlich auch gut in einem getrennten Abschnitt untergebracht werden, wirken sich aber besonders in diesem Kontext aus, weswegen sie hier eingefügt wurden. In einer zukünftigen Iteration könnten derartige Regelungen in einem Abschnitt „Dokumentations- und Mitteilungspflichten“ überführt werden.

Erläuterung zu § 4 Verhältnis

Dem Charakter eines Mehr-Personen-Verhältnisses entsprechend regelt dieser Abschnitt die Rechtsbeziehungen untereinander, insbesondere werden auch Regelungen zur gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO getroffen, so dass bei Fehlen einer Absprache der Parteien untereinander hier eine Rückfalloption besteht. Eine detailliertere Vereinbarung ist aber in der Regel zu empfehlen.
Gleichzeitig sieht der Abschnitt Möglichkeiten zur Bevollmächtigung von sowohl Hauptverantwortlich Datengebenden als auch FDZ vor, was Vertragsanpassungen erleichtern soll. Welche Vollmachten im konkreten Kontext sinnvoll sind, dürfte von den Spezifika des Vorhabens, der Beteiligten und der Sensitivität der Datenbasis abhängen. In der Regel dürften aber alle Bevollmächtigungen sinnvolle Vereinfachungen darstellen.

Erläuterung zu § 5 Veröffentlichungen von Ergebnissen

Klauseln zur Veröffentlichung waren in allen Verträgen enthalten. Die hier vorgesehenen Regelungen stellen eine Vermittlungsversuch dar, der hoffentlich für alle akzeptabel ist. So wollten manche Einrichtungen 3, aber die meisten 1-2 Belegexemplare von Veröffentlichungen. Der Vorschlag geht hier den Mittelweg.
Über eine weite Definition in der Begriffsbestimmung sollen alle Fälle erfasst werden, in denen ein Risiko besteht, dass über eine Veröffentlichung Elemente der Datenbasis in schriftlicher Form in die Öffentlichkeit gelangen.
An sie knüpft über die entsprechende fakultative Klausel in den TOMs die Pflicht der Freigabe vor Veröffentlichung an.
Um allerdings die praktischen Interessen der Datennutzenden nicht aus dem Blick zu verlieren, besteht die Möglichkeit rein interne Zwischenberichte aus dem Anwendungsbereich herauszunehmen.
Um der Anforderung nach teilweise sehr spezifischen Zitationsregeln einzelner Institutionen gerecht zu werden, besteht hierfür die Möglichkeit, diese in einem getrennten Anhang zu definieren. In der Regel sollte aber ein genereller Verweis auf die wissenschaftliche Praxis genügen; zumal spezifische Vorgaben auch mit disziplinären Vorgaben kollidieren können.

Erläuterung zu § 6 Datenschutzrechtliche Pflichten und Garantien

In Anlehnung an die Struktur der Standard-Datenschutzklauseln der EU-Kommission sind in diesem Abschnitt die datenschutzrechtlichen Maßgaben des Vertrages konzentriert. Auf diesem Weg sollte die Kombination/Erweiterung gut darstellbar sein, indem einfach am Ende die entsprechende Option gewählt und der Anhang einbezogen wird.
Es ließ sich nicht ganz vermeiden stellenweise Aspekte anderer Regelungsbereiche jenseits des Datenschutzes hier zu integrieren, weil sie im Kontext sinnvoll hier zu regeln waren.

Erläuterung zu a) Zweckbeschränkung

Die Bestimmung zur Zweckbeschränkung stellt im Grunde eine Redundanz dar, ist hier aber aufgrund der herausragenden Bedeutung des Zweckbindungsprinzips in der DSGVO und der besseren Komplementarität zu den Standardklauseln dennoch aufgenommen worden.

Erläuterung zu b) Transparenz

Auch der Verweis auf Art. 12ff DSGVO ist eigentlich redundant, da er sich ja bereits aus dem Gesetz ergibt. Ähnlich wie im vorigen wurde sie dennoch aufgenommen um die Vorschriften in Erinnerung zu rufen.
Auf eine Regelung zur Publikation der auf den Datenbeständen basierenden Veröffentlichungen wurde verzichtet, weil es diesbezüglich keiner vertraglichen Regelung bedarf. Die Zusammenstellung von Publikationslisten kann unproblematisch auf das berechtigte Interesse des FDZ gestützt werden. Es besteht allenfalls eine Mitteilungspflicht, gem. Art. 13, 14 DSGVO, der mit der o.g. Regelung genüge getan wird. Auch die Möglichkeit eines Widerspruchs etwa bei Bachelorarbeiten wurde abgebildet.
Es folgen Bestimmungen zur Speicherung durch das FDZ, wobei die fakultativen Klauseln mit Hinweisen auf die entsprechenden Betroffenenrechte ausgestattet wurden.
In manchen Fällen gebietet die DSGVO in ihren Transparenzerfordernissen auch die Zugriffsberechtigung zugänglich zu machen, hierfür wird mit der fakultativen Klausel Rechnung getragen.

Erläuterung zu c) Richtigkeit und Datenminimierung

Die Richtigkeit ist im Datenschutzrecht Charakter eines Grundsatzes, weswegen dieser Aspekt in diesem Abschnitt Erwähnung findet. Er enthält aber auch Regelungen, die – jenseits des Datenschutzrechtes – Rücktrittsmodalitäten bei Mängeln formuliert. Zur Vermeidung von Doppelungen in der Gliederung wurde diese Regelung hier eingefügt.

Erläuterung zu d) Dauer

Die Löschverpflichtung ist in allen Vertragsmodellen in dieser oder ähnlicher Form enthalten. Dem Bedenken, dass eine spätere Überprüfung der Einhaltung der guten wissenschaftlichen Praxis durch die Löschung verunmöglicht wird, wird durch die Archivierungsverpflichtung und eine entsprechende Regelung im Rahmen der Bestimmungen zur Weiterübermittlung Rechnung getragen.
Eine Klausel zur Löschung mathematisch veränderter Daten war nur in einem Vertrag enthalten, dürfte aber bei quantitativen Analysen regelmäßig sinnvoll sein. Sie wurde daher in die Muster-TOMs übernommen. Der Dokumentation der Berechnungen dürfte in diesen Fällen nur durch die Dokumentation der eingesetzten Algorithmen Rechnung getragen werden, aber nicht durch Dokumentation der Datenbasis oder etwaiger Zwischenergebnisse. Dies könnte durchaus problematisch sein und ist ggf. in einer zukünftigen Version noch zu verfeinern. Möglicherweise bestünde ein sinnvolle Lösung darin, die Derivate durch das FDZ zu archivieren.

Erläuterung zu e) Sicherheit der Datenverarbeitung

Dieser Abschnitt bezieht vor allen Dingen auf den Anhang zu Technischen und Organisatorischen Maßnahmen, enthält aber darüber hinaus eine Regelung, diese, wo erforderlich, an den Stand der Technik anzupassen. Damit sind auch Fälle von sog. „Zero-Days“, also kurzfristig auftauchenden Angriffen auf IT-Systeme schon im Vertrag besonders Rechnung getragen.

Erläuterung zu f) Besondere Kategorien von Daten

Auch die Anforderungen an die Verarbeitung sog. sensibler Daten ist in der Regel durch die TOMs Rechnung zu tragen – sofern eine Verarbeitung überhaupt zulässig ist.

Erläuterung zu g) Beschränkung der Zugriffsberechtigten, Weiterübermittlung

Bezüglich der Zugriffsberechtigten verfolgt der Vertrag grundsätzlich einen restriktiven Ansatz. Ohne Fakultativklauseln sind nur die Vertragsparteien zur Verarbeitung berechtigt. In der Praxis werden aber oftmals auch Mitarbeitende an Lehrstühlen etwa mit der Vorbereitung von Daten befasst werden, was durch die Fakultativklausel ermöglicht wird.
Dem Fall der Überprüfung im wissenschaftlichen Kontext wurde mit einer eigenen Bestimmung Rechnung getragen.

Erläuterung zu h) Auftragsverarbeitungen

Die Einschaltung von Dienstleistern im Rahmen von Auftragsvereinbarungen durch die Datennutzenden unterliegen stets der Pflicht der Zustimmung durch den Datengeber; ggf. könnte hier auch eine Widerspruchsvariante überlegt werden. Die vorgeschlagene Regelung war allerdings in der Praxis absolut vorherrschend.

Erläuterung zu i) Unterstützungspflichten

Die Prüfung der Einhaltung der Vertragsbedingungen ist Ausdruck des Prinzips der Rechenschaftspflicht. Die erforderliche Tiefe der Prüfungskompetenz ist nicht gesetzlich vorgeschrieben; die Verträge sahen diesbezüglich teilweise recht weitreichende Befugnisse vor, wie in den fakultativen Klauseln zum Ausdruck kommt. Aufgrund Ihres invasiven Charakters dürften sie nur in Ausnahmefällen relevant werden.
In Anlehnung an einige Musterverträge wurde auch ein Hinweis auf die Aufsichtsbehörden aufgenommen. Sie erscheint rein deklaratorischer Natur, da sich die Befugnisse bereits aus dem Gesetz ergeben. In einem Fall, sind dies ausweislich der Vertragsbeispiele auch der BRH (vgl. etwa §104 BHO) und andere, neben den Datenschutzaufsichtsbehörden, genannt.
Bei Drittstaatsbezug im internationalen Datentransfer gilt über die Standardvertragsklauseln zusätzlich eine Unterwerfung unter die Befugnisse der Datenschutzaufsichtsbehörden.

Erläuterung zu j) Drittbegünstigung

Diese Regelung ergibt sich aus der Drittbegünstigungsklausel der Standardverträge der EU-Kommission bei internationalen Datenübermittlungen, weswegen sie hier auch als fakultative Klausel für Sachverhalten ohne Drittstaatsbezug aufgenommen wurde. Sie ist nicht ganz unproblematisch, weil diese Pflichten für die Datennutzenden nicht immer vollumfänglich transparent sind. Es mag aber sein, dass Datengebende Stellen entsprechende Pflichten gegenüber den Betroffenen haben; in diesen Fällen sollte sie einbezogen werden.

Erläuterung zu k) Internationale Datenübermittlungen

Die Übermittlung in Drittstaaten ist nach Art. 46 Abs. 2 lit c) DSGVO zulässig, wenn sie auf Grundlage der von der EU-Kommission erlassenen Standardvertragsklauseln erfolgen (vgl. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de).
Daher sind diese bei beabsichtigten Drittstaatsübermittlungen einzubeziehen.
Andere Formen der zulässigen Drittstaatsübermittlung – etwa über Einwilligungen seitens der Betroffenen oder über verbindliche unternehmensinterne Datenschutzvorschriften deckt dieser Vertrag derzeit nicht ab.

Erläuterung zu § 7 Vertragsverstöße und Haftung

Das Sanktionssystem bei Datennutzungsverträgen ist – auch weil noch keine Empirie zur Anwendung vorliegt – sicher noch weiterentwicklungsfähig. Entsprechend der verbreiteten Praxis wurden zunächst einige Vertragsverstöße exemplarisch hervorgehoben.

Als Sanktionsinstrument bei Vertragsverstößen werden zunächst nicht pekuniäre Mechanismen eröffnet; lediglich als „last resort" wird auch die Zahlung einer Geldstrafe relevant, wobei hier bezüglich der Höhe auf den in anderen Bereichen etablierten „Hamburger Brauch" zurück gegriffen wird, der ermöglicht die Höhe Vertragsstrafe auf die Umstände des konkreten Vertragsverstoßes anzupassen.

Die Haftungsregelungen beschränken die Haftung von FDZ und Datengebender Stelle auf ein Minimum, was aber im Kontext auch angemessen erscheint.

Erläuterung zu § 8 Sonstiges

Hinzuweisen ist hier insbesondere auf den Punkt b) Änderungen: Nach dem Vertragsmuster sind Änderungen im Hauptvertrag nur schriftlich möglich, allerdings sind die Sachverhalte, die in den Anhängen geregelt sind, auch in Textform (§126b BGB) möglich, das heißt auch z. B. per E-Mail. Um die Form der Anhänge zu wahren, können diese etwa als PDF im Anhang zirkuliert werden, was auch die einheitliche Dokumentation erleichtert.

Erläuterung zu Anhang Datennutzende

Dieser Anhang sollte für jede/n Datennutzenden getrennt auszufüllen; für die Datennutzenden, die schon bei Vertragsschluss bekannt sind, kann auch eine Tabelle geführt werden, die jeweils die Bezeichnung, Adresse und eine Unterschrift der beitretenden enthält; wobei dies nur bei einer großen Zahl von Datennutzenden (etwa: Seminarteilnehmende) sinnvoll erscheint.

Erläuterung zu Anhang Datenbasis

Der Bezeichnungsweise der Datenbasis ist organisationsspezifisch; entsprechende Hinweise sollten in diesem Anhang beschrieben werden.

Erläuterung zu Anhang Datenzugang

Der modus operandi des Datenzugangs ist organisationsspezifisch; entsprechende Hinweise sollten in diesem Anhang beschrieben werden.

Erläuterung zu Anhang Kostenmodell

Die Kostenmodelle sind organisationsspezifisch; entsprechende Hinweise sollten in diesem Anhang beschrieben werden.

Erläuterung zu Anhang Zitationsregeln

Einige Organisationen/FDZ sehen sehr spezifische Zitationsregeln vor; entsprechende Vorgaben sollten in diesem Anhang beschrieben werden.

Erläuterung zu Anhang EU-Standardvertragsklauseln

Die EU-Standardvertragsklauseln sind in getrenntem Dokument geführt, weil sei eine eigene Nummerierungssystematik vorgeben. Siehe auch: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de.

Erläuterung zu Anhang Spezifische Einschränkungen der Verarbeitung

Einige Organisationen müssen aufgrund ihres Datenbestandes sehr spezifische Vorgaben zur Verarbeitung machen. Etwa zur Granularität der Berechnungen bei remote execution oder zu spezifischen Zweckbeschränkungen.
Sofern diese Vorgaben nicht bereits im Anhang Technische und organisatorische Maßnahmen oder andernorts dargestellt werden können, sind diese hier aufzunehmen.

Erläuterung zu Unterschriften weiterer Vertragsparteien

Nur erforderlich sofern keine Vertretungsbefugnis seitens FDZ und Hauptverantwortlich Datennutzenden besteht (vgl. entsprechende Klausel im Hauptvertrag). Andernfalls ist diess Zeile für jede weitere nicht vertretene Vertragspartei zu kopieren und anzupassen.

Erläuterung zu Anhang Datenbasis

Der Bezeichnungsweise der Datenbasis ist organisationsspezifisch; entsprechende Hinweise sollten in diesem Anhang beschrieben werden.

Erläuterung zu Anhang: Vertragserweiterung, hier Unterschriften weiterer Vertragsparteien

Nur erforderlich sofern keine Vertretungsbefugnis seitens FDZ und Hauptverantwortlich Datennutzenden besteht (vgl. entsprechende Klausel im Hauptvertrag). Andernfalls ist diess Zeile für jede weitere nicht vertretene Vertragspartei zu kopieren und anzupassen.

Erläuterung zu Anhang: Datennutzende

Die Vertragserweiterung ist für jede/n Datennutzenden getrennt auszufüllen.

Erläuterung zu „Datengebende Stelle gleichzeitig Forschungsdatenzentrum (FDZ)“

Bitte ankreuzen (x) bei datenschutzrechtlicher Verantwortlichkeit des FDZ.

Erläuterung zu „in Vertretung für die Datengebende Stelle“

Sofern das FDZ durch den Hauptvertrag bevollmächtigt ist im Namen der Datengebenden Stelle eine Erweiterung des Vertrages um weitere Nutzende zuzustimmen, dann muss dies hier gekennzeichnet werden. Sofern das FDZ allerdings selbst als Datengebende Stelle agiert, weil etwa eigene Datenbestände des FDZ verarbeitet werden, oder dem FDZ in getrenntem Vertrag die Datenbestände in die eigene Verantwortlichkeit übermittelt wurden.
Sofern die Datengebende Stelle sich die Zustimmung zur Erweiterung vorbehalten hat (also keiner der o.g. Fälle vorliegt) kann die Vertragserweiterung nur erfolgen, wenn auch sie zeichnet.

Erläuterung zu „Unterschriften weiterer Vertragsparteien“

Nur erforderlich sofern keine Vertretungsbefugnis seitens FDZ und Hauptverantwortlich Datennutzenden besteht (vgl. entsprechende Klausel im Hauptvertrag). Andernfalls ist diess Zeile für jede weitere nicht vertretene Vertragspartei zu kopieren und anzupassen.

Fragen und Antworten zu Datennutzungsverträgen

(Alle Fragen bezogen sich auf die Annahme, dass die Musterverträge gelten.)

1 ID in Panelprojekten

1.1 Allgemein

Das Problem bei einem Panelprojekt ist, dass es immer eine Liste geben muss, mit dem ein Umstieg des Personencodes (im getrennten) Datensatz und den personenbezogenen Daten beim Befragungsinstitut oder beim eigenen Institut möglich ist.

a. Streng genommen könnte man argumentieren, dass ein laufendes Panel nie anonym sein kann (auch wenn alle anderen Angaben stark anonymisiert[1] wurden), sondern nur pseudonym. Ist das korrekt? Es wird um Erläuterung gebeten.

Antwort:
Das ist zutreffend. Pseudonyme Daten im sind stets auch personenbezogene Daten und unterliegen damit der DSGVO.
Bei „starker Anonymisierung" der Angaben, im Sinne der Definition der Fußnote 1, die im Einzelfall mitunter schwer herstellbar ist (siehe hierzu auch unten zu den Begriffen „absolute Anonymisierung" und „faktische Anonymisierung" unter 2.1), handelt es sich bei Panelprojekten um eine Pseudonymisierung im Sinne der Definition des Art. 4 Nr. 5 DSGVO.
Diese Definition geht davon aus, dass der verbleibende Datenbestand keine Personenbeziehbarkeit mehr aufweist, sondern der Personenbezug nur (und ausschließlich) über die Personencodes hergestellt werden kann.
In der Regel wird allerdings den Daten im verbleibenden Datenbestand ein gewisses Maß an Personenbeziehbarkeit erhalten bleiben, weswegen die Anforderung der o.g. Definition der DSGVO nicht in allen Fällen erfüllt sein wird, auch wenn dies landläufig ebenfalls (und durchaus berechtigterweise) als Pseudonymisierung bezeichnet wird. Schon daher ist auch dieser Datenbestand wirksam zu schützen. In jeder Variante können Pseudonymisierungen (also auch jene, bei der die Restdaten nicht absolut anonym sind) eine gute technische Maßnahme darstellen, die die Risiken der Datenverarbeitung deutlich minimiert.
Entsprechend bleibt bei jeder Form der Pseudonymisierung die Anwendbarkeit der DSGVO bestehen. Allerdings können die Anforderungen, die an weitere technische und organisatorische Maßnahmen zu stellen sind, nach einer Pseudonymisierung mitunter deutlich verringert werden.

[1] sodass aus keiner Kombination von Angaben Einzelpersonen identifiziert werden können.

1.2 Übermittlung ins Ausland

a. Bitte berücksichtigen Sie hier die Antwort aus 1.1.a: Darf man diese Daten (s. 1.1 a.) in die USA oder in andere Drittstaaten übermitteln, bzw. was ist hier zusätzlich notwendig?

b. Gibt es einen Unterschied zwischen einer Übermittelung in die USA und anderen Drittstaaten?

Antwort:
Die Übermittlung personenbezogener Daten (also auch pseudonymer Daten, siehe oben 1.1.a) in Drittstaaten (außerhalb des Europäischen Wirtschaftsraums, d.h. den EU-Mitgliedsstaaten sowie Norwegen, Liechtenstein und Island) unterliegt nach der DSGVO den besonderen Vorschriften des Kapitel V. Sie darf nur erfolgen, wenn mindestens eine der in diesem Kapitel genannten Varianten einschlägig ist. Diesbezüglich ergeben sich auch für die USA keine Besonderheiten.
Für Datenübermittlungen im Wissenschaftskontext sind insbesondere folgende Varianten besonders hervorzuheben:

1. *Datenübermittlungen in Länder, für die ein Angemessenheitsbeschluss nach Art. 45 DSGVO durch die Kommission vorliegt, sind wie Übermittlungen innerhalb der EU zu behandeln.*[2] *Zurzeit sind dies:*
   - *Andorra*
   - *Argentinien*
   - *Kanada (für kommerzielle Organisationen, die dem "Personal Information Protection and Electronic Documents Act" unterliegen)*
   - *Färöer*
   - *Guernsey*
   - *Israel*
   - *Insel Man (Isle of Man)*
   - *Japan*
   - *Jersey*
   - *Neuseeland*
   - *Schweiz*
   - *Uruguay*
   - *das Vereinigte Königreich*

   Diesbezüglich gab es für die USA eine Sonderregelung (sog. „safe-harbour-Regelung", später: „Privacy Shield"), die aber durch den EuGH in der Entscheidung „Schrems II" aufgehoben wurde, so dass auf Art. 45 DSGVO vorerst bei Übermittlungen in die USA nicht zurückgegriffen werden kann.

2. *Art. 46 DSGVO ermöglicht die Datenübermittlung vorbehaltlich geeigneter Garantien, wozu u.a. die sog. Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit c) zählen. Unter Einbeziehung dieser, von der Kommission erstellten Klauseln,*[3] *die die gesetzlichen Garantien der Länder mit Angemessenheitsentscheidung ersetzen, soll eine Datenübermittlung zulässig sein.*
   Der erstellte Mustervertrag ist so ausgestaltet, dass eine Einbeziehung der Standardvertragsklauseln über einen Vertragsanhang möglich ist.

3. *Schließlich kann die Übermittlung auch auf eine explizite Einwilligung zum Transfer in Drittstaaten gestützt werden, wobei hierbei auf die spezifischen Risiken des Drittstaatstransfers hingewiesen werden muss.*

[2] Für eine Übersicht der bestehenden Angemessenheitsbeschlüsse: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de
[3] Siehe: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

2 Datenbereitstellung

2.1 Über unterschiedliche Zugangswege (s. Glossar)

a. Wie kann man datenschutzrechtlich begründen, warum man unterschiedlich stark anonymisierte Daten unterschiedlich rausgeben kann? (z. B. stark anonymisierte Daten via Download, weniger stark anonymisierte Daten On-Site)
b. Wie kann man datenschutzrechtlich begründen, wie stark man die Daten für die unterschiedlichen Zugangswege anonymisieren muss?
c. Kann man diese folgende Argumentation auf die DSGVO anwenden (Download versus Remote-Access-Verfahren)?

> *„[…] Remote-Access-Verfahren eröffnen weitere Variationen beim Zugang zu sensiblen Forschungsdaten. Im Vergleich zu SUF im kontrollierten und verschlüsselten Download bietet Remote Access einen höheren Sicherheitsstandard. Somit können SUF im Remote Access mehr Detailinformationen beinhalten (d. h. weniger stark anonymisiert sein). Faktische Anonymität ist durch die Einhaltung der Regelung, dass Einzelangaben „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft [...] zugeordnet werden können“ (BDSG §3 (6)) weiterhin gewährleistet. Somit ist die faktische Anonymität von Forschungsdaten stets in Bezug auf […] [die] Anonymisierung und [den] Datenzugangsweg) zu sehen […]“*

Quelle: https://www.konsortswd.de/wp-content/uploads/RatSWD_WP_261.pdf, S. 5

Es gibt eine Stellungnahme des Bundesdatenschutzbeauftragten vom 10.2.2020. Dort schreibt er mit Bezug zur DSGVO: „Eine absolute Anonymisierung derart, dass die Wiederherstellung des Personenbezugs für niemanden möglich ist, dürfte häufig nicht möglich sein und ist im Regelfall datenschutzrechtlich auch nicht gefordert. Ausreichend ist in der Regel, dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften wiederhergestellt werden kann.“
Quelle:
https://www.bfdi.bund.de/SharedDocs/Konsultationsverfahren/2020/01_Anonymisierung-TK.pdf?__blob=publicationFile&v=6
Dies wiederum entspricht inhaltlich in etwa der alten Definition von faktischer Anonymität im Rahmen des BDSG.

Antworten zu a)-c):

Sofern absolute oder – zumindest in Teilbereichen – auch faktische Anonymisierung[4] vorliegt, gilt das Datenschutzrecht nicht, weil keine Personenbeziehbarkeit mehr besteht.

Da die Abgrenzung jedoch schwierig ist, und sich in vielen Fällen nicht gänzlich ausschließen lässt, dass der Datenbestand noch personenbeziehbare Daten enthält, gilt die DSGVO. In diesem Fall spielt die Anonymisierung in der Wissenschaft als Maßnahme der Datenminimierung eine Rolle, die in Art. 89 DSGVO gefordert ist, um insbesondere im Rahmen des Verweises aus Art. 5 Abs. 1 lit. b) DSGVO wissenschaftliche Datenverarbeitungen als vereinbar mit dem ursprünglichen Zweck zu bewerten; diese „Zweckvereinbarkeitsfiktion" eröffnet dann über Art. 6 Abs. 4 DSGVO die Weiterverarbeitung, wobei diese in manchen Fällen auf ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f) gestützt werden wird, der wiederum eine Interessensabwägung vorsieht, bei der die Risikoreduktion der Anonymisierung, aber auch der etwa durch verschiedene Zugangswege berücksichtigt werden kann.

Die Anforderung unterschiedlich starke Anonymisierungen durchzuführen, lässt sich also datenschutzrechtlich an verschiedenen Stellen in der DSGVO verorten. Eine klare, eindeutige Vorgabe, wann „remote access" und wann „download" zulässig ist, macht die DSGVO nicht. Es handelt sich dabei um Verfahren zur Risikominimierung, die insbesondere aus Gründen des Datenschutzes durch Technikgestaltung in Art. 25 DSGVO vorgeschrieben sind:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen."*

[4] Der Begriff „Anonymität" und „Anonymisierung" ist in der DSGVO nicht definiert, allerdings werden die Begriffe in Erwägungsgrund 26 verwendet:

> „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann."

Demnach soll also die DSGVO nicht für Daten gelten, die in einer Form anonymisiert worden sind, dass keine Identifizierung mehr möglich ist, was auch als „absolute" Anonymität bezeichnet wird. Wie aus der Stellungnahme des BfDI deutlich wird, ist das allerdings die Ausnahme. Daher muss man davon ausgehen, dass es auch Anonymisierungen gibt, die diese Anforderung nicht absolut erfüllen. In einem Übergangsbereich sind „faktische" Anonymisierungen anzusiedeln, wie sie vom BfDI beschrieben werden, bei denen die DSGVO eigentlich auch nicht anwendbar sein soll, weil der Aufwand unverhältnismäßig zur Deanonymisierung wäre. Problematisch ist hieran, dass es mE bislang keine einheitlichen anerkannten Verfahren gibt, nach der sich beurteilen lässt, wann dieses Niveau faktischer Anonymität erreicht ist, zumal mit der Zeit, Datenbestände die zunächst als faktisch anonym eingeordnet werden konnten, zu einem späteren Zeitpunkt – etwa wegen höherer verfügbarer Rechenleistung oder neuem, zugänglich Zusatzwissen, diese Qualitätsstufe nicht mehr erreichen. Es ist daher empfehlenswert – zumindest in Grenzbereichen - von der Anwendbarkeit der DSGVO auszugehen; die Anonymisierung stellt dann eine technische Maßnahme zur Risikoreduktion dar.

2.2 in Drittstaaten

FDZ bekommen auch Anfragen zur Datenbereitstellung (z. B. Download von Daten) außerhalb der EU bzw. EWR (EU plus Island, Liechtenstein sowie Norwegen).

a. Was muss hier bei der internationalen Datenbereitstellung bedacht werden, wenn die Daten nur in Länder mit einem Datenschutzniveau ähnlich der DSGVO weitergegeben werden sollen?

Antwort:
Siehe oben, Antwort zu 1.2. Sofern eine „Adäquanzentscheidung" der EU-Kommission bezüglich des Landes besteht oder es sich um ein EWR/EU-Staat handelt, sind keine Besonderheiten zu beachten.

b. Muss im Vertrag explizit stehen, dass die Download-Daten im EWR oder der EU bleiben müssen, wenn die Daten nur in Länder mit einem Datenschutzniveau ähnlich der DSGVO weitergegeben werden sollen?

Antwort:
Das ist zu klarstellend zu empfehlen, es ergibt sich aber auch schon direkt aus der DSGVO (Art. 44 Abs. 1 Satz 1).

c. Angenommen, die Daten sind vor dem Hintergrund der DSGVO erhoben und anonymisiert. Können diese Daten weltweit zur Verfügung gestellt werden oder sind teilweise weitere Regelarien zu beachten? Wenn ja, welche?

Antwort:
Wenn es sich um absolut anonymisierte Daten handelt, oder im o.g. Sinne „faktische" Anonymität erreicht wurde, dann können die Daten aus Sicht der DSGVO weltweit zur Verfügung gestellt werden; die DSGVO gilt für diese Daten nicht.

Sofern aber keine Sicherheit über die Anwendung der DSGVO besteht, weil man nicht sicherstellen kann, dass doch noch eine DSGVO-relevante Personenbeziehbarkeit besteht, ist eine Übermittlung in Drittstaaten nur unter Einhaltung der Anforderungen von Kapitel V der DSGVO möglich (siehe oben 1.2).

d. Angenommen, die Daten sind vor dem Hintergrund des Sozialgesetzbuchs (SGB) erhoben und anonymisiert. Können diese Daten weltweit zur Verfügung gestellt werden oder sind teilweise weitere Regelarien zu beachten? Wenn ja, welche?

Antwort:
Sofern mit der Frage auf die Regelungen des Sozialgeheimnis Bezug genommen i.S.v. § 35 SGB I Bezug genommen wird, gilt Folgendes:
Das Sozialgeheimnis verweist in seiner Definition auf die Regelungen der DSGVO zum Personenbezug, betrifft aber darüber hinaus auch Daten, die dem Betriebs- und Geschäftsgeheimnis unterfallen. Sofern die Daten wirksam anonymisiert sind und keine Betriebs- und Geschäftsgeheimnisse betroffen sind, gilt das Sozialgeheimnis nicht.
Bei Anonymisierungsverfahren, bei denen nicht sicher davon auszugehen ist, dass eine faktische Anonymisierung im o.g. Sinne gegeben ist, gilt neben den Anforderungen der DSGVO insbesondere die Einschränkung der wissenschaftlichen Verarbeitung nach § 67c Abs. 5 SGB X, wonach

> *„von den in § 35 des Ersten Buches genannten Stellen nur für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der Planung im Sozialleistungsbereich verändert oder genutzt werden [dürfen]“.*

Darüber hinaus sieht § 75 SGB X einen Genehmigungsvorbehalt für Forschung mit Sozialdaten vor; diese Genehmigung kann auch die Forschung durch nichtöffentliche Stellen einschließen, wenn die Genehmigungsvoraussetzungen vorliegen. Die Übermittlung in Drittstaaten ist in den Genehmigungsanforderungen nicht ausdrücklich ausgeschlossen, was darauf hindeutet, dass eine Übermittlung – unter Einhaltung der Anforderungen des Kapitel V DSGVO, s.o. – grundsätzlich möglich ist.
Allerdings stellen sich hier eine Reihe von Problemen: Zunächst muss ein öffentliches Interesse der Forschung bestehen, das das Geheimhaltungsinteresse der Betroffenen erheblich überwiegt. Aufgrund der Risikoerhöhung bei einem Drittstaatstransfer, könnte diese erhöhte Abwägungsanforderung schwer erfüllbar sein. Zudem unterwirft § 75 Abs. 6 SGB X den Datenempfänger der Aufsicht durch die Landesaufsichtsbehörden, was schon im innereuropäischen Kontext Fragen aufwirft.

e. In welche Länder können die Daten als Download bereitgestellt werden, wenn die Daten nur in Länder mit einem Datenschutzniveau ähnlich der DSGVO weitergegeben werden sollen? Könnte man diese Liste als Grundlage nutzen oder gibt es Alternativen? https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Antwort:
Die Liste kann und sollte als Grundlage herangezogen werden. Eine Alternative auf Ebene ganzer Staaten gibt es nicht.

f. Können im Falle des Musterdatennutzungsvertrags auch Personen Daten in Drittstaaten als Download angeboten werden?

Antwort:
Ja, sofern die Standarddatenschutzklauseln der EU-Kommission einbezogen werden (siehe oben). Der Vertrag ist so ausgelegt, dass dies einfach möglich ist.

g. Manche FDZ handhaben die Datenbereitstellung derart, dass in Drittstaaten keine Daten via Download bereitgestellt werden, sondern nur via Remote-Desktop, d. h. die Daten bleiben auf deren Servern, die User*innen können die Daten nicht herunterladen. Gibt es dafür eine rechtliche Begründung?

Antwort:
Ja und Nein: Ausdrücklich ist das nicht in der DSGVO geregelt. Auch ein Zugriff über ein Remote-Desktop ist als Drittstaatsübermittlung anzusehen. Allerdings reduziert der remote-Desktop-Zugriff die Risiken der Datenverarbeitung, weswegen dies eine sinnvolle Maßnahme sein kann, um mit den spezifischen Risiken der Drittstaatsübermittlung umzugehen.

3 Löschungsanzeigen bei Download-Dateien für einen bestimmten Nutzungszeitraum

Datennutzer*innen werden Datensätze zum Download bereitgestellt, die sie nur für ein angegebenes Projekt zu einem angegebenen Zeitraum nutzen dürfen.

a. Wird eine schriftliche Bestätigung benötigt, dass die Nutzer*innen die Daten sowie Kopien und Auszüge von allen Datenträgern gelöscht haben oder reicht ein Verweis auf diese Verpflichtung im Datennutzungsvertrag, ohne dass eine Löschungsanzeige eingefordert wird?

Antwort:
Die Frage nach der Pflicht einer Löschanzeige ist leider nicht einfach zu beantworten.
Nach meiner Auffassung ergibt sich so eine Pflicht nicht direkt aus der DSGVO. Vielmehr kann eine vertragliche Pflicht die Löschung zu bestätigen, als technische und organisatorische Maßnahme eingeordnet werden, die die Risiken der Verarbeitung reduziert. Sie ist damit wie alle technischen und organisatorischen Maßnahmen

> *„unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ (Art. 24 Abs. 1 DSGVO)*

geboten. Es kann also mittelbar durchaus eine Pflicht bestehen, eine solche Maßnahme zu ergreifen.

Die DSGVO schreibt vor, dass datenverarbeitende Stellen für die Einhaltung der Bestimmungen rechenschaftspflichtig sind. Zu diesen Bestimmungen zählt die Löschverpflichtung, die gemäß dem Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e) DSGVO auch im Forschungsbereich gilt (auch wenn dort eine Verlängerung der Speicherung gegenüber etwaigen ursprünglichen Zwecken eingeräumt wird). Damit sind sowohl datengebende Stellen wie Nutzende zur Löschung schon per Gesetz verpflichtet (und gleichzeitig auch zur Dokumentation der Löschung). Einer vertraglichen Regelung würde es daher eigentlich gar nicht bedürfen, obschon sie sicherlich dem Gesetz Nachdruck verleihen kann und eine gute Erinnerungsfunktion hat.
Allerdings sind – wie oben dargestellt – technische und organisatorische Maßnahmen zur Einhaltung der DSGVO zu ergreifen. Eine vertragliche Bestätigungspflicht der Löschung kann hier eine wirksame Maßnahme zur Risikoreduktion darstellen, bei der man im Einzelfall auch die Auffassung vertreten könnte, dass sie wegen Art. 24 Abs. 1 DSGVO in bestimmten Fällen zwingend im Vertrag vorzusehen ist. In welchen Fällen das gelten mag, lässt sich derzeit noch nicht abschließend sagen.

b. Wenn ein Verweis auf diese Verpflichtung im Datennutzungsvertrag ausreicht, wie müsste die Formulierung im Datennutzungsvertrag heißen?

Antwort:
Siehe Mustervertrag, der beide Varianten vorsieht.

c. Falls ein Verweis auf diese Verpflichtung im Datennutzungsvertrag nicht ausreicht

   i. Welche rechtlichen Folgen hat es im Falle des im Rahmen dieser Vergabe zu erstellenden Mustervertrags, wenn Nutzende nicht mehr unter der angegebenen Kontakt E-Mail erreichbar sind (obwohl sie die hätten aktualisieren müssen).

Antwort:
Hierbei handelt es sich um einen Vertragsverstoß, der als Verletzung vertraglicher Nebenpflichten zu qualifizieren sein wird und nach §§ 280 I, 241 II BGB Schadenersatzansprüche auslösen kann. Daher sollte stets neben der E-Mail auch eine (ladungsfähige) Anschrift in den Vertrag aufgenommen werden.

ii. Reicht es im Falle des im Rahmen dieser Vergabe zu erstellenden Mustervertrags, dass der rechtlichen Pflicht nachgekommen wurde, indem dazu aufgefordert wurde?

Antwort:
Nein, wenn die Löschanzeige unter den Bedingungen von Art. 24 Abs. 1 DSGVO als Maßnahme für geboten gehalten wird, wird eine Aufforderung die vertraglich ausbedungene Bestätigung zu erbringen, nicht ausreichen. Die vertraglichen Pflichten müssen im Rechtswege durchgesetzt werden, weil ansonsten Zweifel an der Wirksamkeit der Maßnahme bestehen könnten.

4 Vertragsstrafe

4.1 Alternative zu Vertragsstrafe?

Manche (internationale) Organisationen möchten keinen Datennutzungsvertrag abschließen, da sie eine Vertragsstrafe enthält.

a. Gibt es eine Alternative zur Vertragsstrafe, um die Relevanz der Vertragsverpflichtung zu unterstreichen? Wenn ja, welche und welche Unterschiede weist sie auf?
b. Ist es möglich, individuell Vertragsstrafen aus einem Vertrag rauszunehmen?
c. Aus welchen Gründen sind Vertragsstrafen problematisch, insb. bei öffentlichen Institutionen?

Antwort:
Vertragsstrafen sind ein Mittel, der Einhaltung von Verträgen auch unabhängig von eventuellen Schadenersatzansprüchen Nachdruck zu verleihen. Neben der klassischen monetären Vertragsstrafe, drängen sich im vorliegenden Kontext andere Möglichkeiten auf, eine Vertragsverletzung zu ahnden. So ist an die Sperrung weiterer Zugriffe, aber auch an die Weitergabe der Information über die Vertragsverletzung an die Öffentlichkeit, andere Institutionen oder die Aufsichtsbehörden zu denken. Der Mustervertrag sieht hierfür eine Lösung vor, die die monetäre Vertragsstrafe nur noch als letztes Mittel vorsieht.

Eine Pflicht zur Einbeziehung einer Vertragsstrafe kann ich der DSGVO nicht entnehmen. Sie unterliegt insoweit der Vertragsfreiheit und kann individuell verhandelt werden.

Vertragsstrafen können bei Körperschaften des öffentlichen Rechts im Rahmen der Vergabe und des Haushaltsrechts Schwierigkeiten bereiten. Denkbar ist, dass die Zeichnung von Verträgen, die Vertragsstrafen beinhalten, die Kompetenz der ansonsten befugten Mitarbeiterinnen und Mitarbeiter überschreitet und damit den Aufwand erhöht; sie sind aber grundsätzlich auch in Verträgen mit der öffentlichen Hand nicht unüblich (wie auch aus der Berichterstattung bei der PKW-Maut zu entnehmen ist).

4.2 Vertragsstrafe für Privatpersonen?

Es sind teilweise innerhalb FDZ Datennutzungsverträge erstellt worden, sodass Verträge zwischen a) der Institution, die das FDZ betreibt und b) den individuellen Datennutzer*innen abgeschlossen werden können. Dies hat die folgenden Vorteile:

1. Die Datennutzer*innen können/müssen selbst unterschreiben und müssen keine Unterschriften von Vorgesetzten/Verwaltungsstellen einholen.
2. Die Verträge bestehen für die Person selbst, so dass sie damit nicht abhängig von Vorgesetzten oder Promotionsbetreuer*innen sind.
3. Institutionenwechsel (Arbeitsplatzwechsel, Arbeitsplatzverlust, Wechsel von Betreuungsverhältnissen bei Promotionen) haben keinen Einfluss auf die Gültigkeit laufender Datennutzungsverträge.

Dennoch enthalten diese Verträge auch Vertragsstrafen etc. Teils wird von Datennutzenden versucht, die Vertragsstrafen aus dem Vertrag streichen zu lassen. Jedoch wird dies auch als Teil des Sicherheitskonzepts verstanden, um den Datennutzenden die Relevanz der Einhaltung der Vertragsbedingungen deutlich zu machen.

a. Gibt es eine Alternative zur Vertragsstrafe, um die Relevanz der Vertragsverpflichtung zu unterstreichen? Wenn ja, welche und welche Unterschiede weisen sie auf?

Antwort:
Vertragsstrafen müssen nicht immer monetärer Natur sein. Eine Reihe der Verträge sieht mit der Meldung von Vertragsverstößen und dem Ausschluss von zukünftigen Zugängen einen anderen Mechanismus (zusätzlich) vor. Der Mustervertrag schlägt hierbei jetzt die monetäre Vertragsstrafe als „letztes Mittel" vor; d.h. nur bei Verstoß gegen die Meldepflicht ist die Vertragsstrafe einschlägig. So kann die Partei, die sonst einer Vertragsstrafe unterworfen ist, die finanzielle Belastung abwenden, ohne dass der Vertragsverstoß frei von Konsequenzen bleibt.

b. Ist eine Vertragsstrafe für eine Privatperson zumutbar/üblich?

Antwort:
Vertragsstrafen gegenüber Privatpersonen sind insbesondere im Rahmen von urheberrechtlichen Unterlassungserklärungen seit vielen Jahren in Deutschland etabliert. Üblich ist hierbei der sogenannte „Hamburger Brauch", wonach

> *„für den Fall einer zukünftig eintretenden schuldhaften Zuwiderhandlung gegen die [zu spezifizierenden] Verpflichtungen eine von der Unterlassungsgläubigerin nach billigem Ermessen festzusetzende, im Streitfall von der zuständigen Gerichtsbarkeit zu überprüfende, Vertragsstrafe an den/die ... (Abmahner eintragen) zu bezahlen."*

Diese Klausel wurde als Variante sinngemäß angepasst in den Mustervertrag aufgenommen. Eine Vertragsstrafe wird demzufolge fällig, wenn nach Abgabe einer solchen Erklärung der erklärenden Person ein weiterer Vertragsverstoß zur Last fällt.

c. Welche Höhe würden Sie ggf. als zumutbar empfehlen?

Antwort:
Die Rechtsprechung hat für Fälle von Vertragsverstößen bei Datennutzungsverträgen noch keine Praxis etabliert. Mir sind bislang keine Urteile zu dieser Frage bekannt. Orientierung kann aber eventuell die Bußgeldpraxis der Aufsichtsbehörden und die sich hier entwickelnde Rechtsprechung geben. Auch aus diesem Grund empfiehlt es sich, dem o.g. „Hamburger Brauch" zu folgen und die Höhe der Vertragsstrafe offen zu lassen und einer gerichtlichen Überprüfung zugänglich zu machen. Andernfalls droht – jedenfalls bei Verträgen mit Privaten ggf., dass die Vertragsstrafenregelung leerläuft.

4.3 Durchsetzung Vertragsstrafe

Angenommen, der im Rahmen dieser Vergabe zu erstellende Mustervertrag gilt. Wie wird praktisch eine Vertragsstrafe durchgesetzt?
Antwort:
Die Durchsetzung der Vertragsstrafe erfolgt, indem die Forderung zunächst geltend gemacht wird und bei Nichtzahlung im Rechtsweg durchgesetzt wird.

5 Institutionswechsel der Datennutzer*in

Datennutzer*innen schießen Datennutzungsverträge mit den Forschungsdatenzentren ab.

a. Angenommen, der Vertrag wurde namentlich mit der natürlichen Person (als der/die Datennutzer*in persönlich) geschlossen. Die Institution wird nicht genannt. Muss dann ein neuer Vertrag geschlossen werden, wenn der/die Datennutzer*in die Institution wechselt?

Antwort:
Nein, in diesem Fall ist die Vertragspartei nicht die Institution; daher muss kein neuer Vertrag geschlossen werden. In der Praxis kann aber die Anbindung an eine Institution durchaus auch für das Vertrauen in die Einhaltung des Vertrags eine wichtige Funktion haben. Der Mustervertrag sieht daher hierfür verschiedene Varianten vor.

b. Angenommen, der Vertrag wurde mit der Institution abgeschlossen und der/die Datennutzer*in möchte nach dem Wechsel der Institution weiter mit den Daten arbeiten. Müsste dann nach dem Wechsel der Institution ein neuer Vertrag mit der neuen Institution (oder dann der Person selbst) abgeschlossen werden?

Antwort:
Ja, in diesem Fall ist die Institution Vertragspartei und zur Datennutzung berechtigt. Die Person ist in diesem Fall bei einem Wechsel der Institution durch den Vertrag zur weiteren Nutzung nicht berechtigt.

6 Institutsinterne Datennutzung

Angenommen, ein Datennutzungsvertrag wird mit den Datennutzenden persönlich und nicht mit deren Institution abgeschlossen.

a. Wenn nun ein/e Mitarbeiter*in der gleichen Institution die Daten nutzen möchte, in dem auch das FDZ angesiedelt ist, wäre es dann angebracht, dass die/der Mitarbeiter*in den gleichen Datennutzungsvertrag abschließt, den auch institutsexterne Datennutzer*innen abschließen?

Antwort:

Beides ist möglich; das Vertragsmuster sieht die Möglichkeit vor, alle in den Vertrag einzubeziehen; es ist aber auch möglich Mitarbeitende über eine interne Verschwiegenheitsverpflichtung Zugang einzuräumen.

b. Müsste dies unterschiedlich abhängig davon beurteilt werden, ob die Datennutzer*in a) persönlich die Daten für eigene Zwecke wie eine Promotion oder einen eigenen Artikel nutzen möchte oder b) die Daten für die Erfüllung einer dienstlichen Aufgabe (bspw. Bearbeitung eines Drittmittelprojektes) benötigt?

Antwort:

Wir empfehlen alle Datennutzenden in den Vertrag einzubeziehen, wobei eine Anbindung an die Institution möglich ist, in diesen Fällen würde ein Wechsel der Institution die Berechtigung entfallen lassen. Es ist aber auch möglich, den Vertrag diesbezüglich (einvernehmlich) zu erweitern.

7 Übersetzung des Vertrags

Es sei angenommen, dass der Gerichtsstand in Deutschland ist. Zudem sei angenommen, ein Datennutzungsvertrag soll für deutschsprachige und englischsprachige Datennutzer*innen verständlich sein. Daher soll der ursprünglich deutschsprachige Vertragstext übersetzt und in Deutsch und Englisch vorgelegt werden können.

a. Soll die englische Übersetzung a) als Lesehilfe zum deutschsprachigen Vertragstext ergänzt werden und die deutschsprachige Fassung als verbindliche Fassung definiert werden (Übersetzung bspw. je Abschnitt oder als gesamt im Anhang)? Oder sollten besser b) zwei getrennte Vertragsfassungen einmal in Deutsch und einmal in Englisch erstellt und jeweils für sich stehend als Vertrag genutzt werden?

Antwort:
Die Frage welche Sprache zur verbindlichen gemacht wird, hängt sicherlich auch von der Präferenz der (datennutzenden) Vertragspartei ab. Üblich ist es wohl in diesen Fällen, die deutsche Fassung verbindlich zu machen und die englische Version als Lesehilfe zur Verfügung zu stellen. Das hat den Vorteil, dass im Fall eines Gerichtsverfahrens Rückübersetzungen und Auslegungen des englischen Textes in der Regel vermieden werden können.

b. Welche Variante wird i.d.R. empfohlen? Was spricht für und gegen die Varianten a) und b)?

Antwort:
S.o. unter lit. a.

8 Aktualisierte Nutzungsbedingungen

Wie müssen Nutzer*innen auf Vertragsverlängerungen, aktualisierte Nutzungsbedingungen (und Kosten) aufmerksam gemacht werden, die sie mit der Registrierung akzeptiert haben?

a. Reicht folgende Formulierung in den AGB solange sich keine wichtigen Punkte wie z. B. Kosten ändern? (was sind wichtige Punkte?)

   „Das XXX behält sich vor diese Datenschutzhinweise von Zeit zu Zeit zu aktualisieren. Wir empfehlen daher, diese Hinweise in regelmäßigen Abständen zur Kenntnis zu nehmen."

   Antwort:
   Die Frage ist etwas unklar. Die Bedingungen des Datennutzungsvertrages sind nach seiner jetzigen Konzipierung nicht einseitig anpassbar. Möglich wäre es, den Vertrag mit einer Sonderkündigungsrechten bei Vertragsänderung(-svorschlägen) auszustatten.
   Sofern sich die Frage auf Datenschutzhinweise auf der Webseite des jeweiligen FDZ bezieht, deren Leistungen nicht durch den Vertrag definiert werden, sind Änderungen möglich. Diese sind lediglich Ausdruck der Transparenzverpflichtung nach Art. 13 DSGVO und allenfalls teilweise Gegenstand des Vertrages.

9 Kosten

a. Dürfen Kosten für die Datennutzung erhoben werden? Auch nur für einzelne Zugangswege oder individuelle Aufbereitungen? Gibt es hier relevante rechtliche Punkte?

Antwort:
Ja, ein Entgelt für die Datenbereitstellung und für den -zugang dürfte in der Regel zulässig sein. Allenfalls in Bereichen in denen IFG-Regelungen unentgeltliche Zugänge zu Informationen vorschreiben, ist dies zu unterlassen. Dies wäre aber dann ohnehin nicht im Anwendungsbereich des Datennutzungsvertrages. Der Anspruch aus Informationsfreiheitsrecht besteht dann neben dem aus dem (kostenpflichtigen) Vertrag.

b. Hängt die Beantwortung der Frage auch von der rechtlichen Grundlage der Institution ab, die das FDZ betreibt (Zuwendung)? (dadurch Vorgaben, Einnahmen/Gebühren nehmen zu dürfen oder auch zu müssen)

Antwort:
Das lässt sich kaum pauschal beurteilen. Dies hängt von den jeweiligen Rahmenbedingungen ab. So können etwa die Zuwendungsbescheide Vorgaben machen, bestimmte Daten und -aufbereitungen kostenfrei oder aber auch explizit kostenpflichtig zugänglich zu machen.