**Einführung in Datennutzungsverträge**

Die Substantive verstehen sich gleichermaßen für alle Geschlechter; lediglich aus Gründen der besseren Lesbarkeit werden die Sprachformen männlich, weiblich und divers nicht verwendet.

1. **Hintergrund zum Bedarf von Datennutzungsverträgen**
   1. “Daten sind das neue Öl” ist ein gebetsmühlenartig wiedergegebener Kommentar zum wirtschaftlichen Hintergrund von Big Data, Machine Learning und dem Technologie-Hype rund um Data Science. Unzweifelhaft sind sehr viele (neue) Businessmodelle unserer Informationsgesellschaft ohne Verarbeitung von Daten schon dem Grunde nach nicht möglich. Oft werden Daten auch zur Optimierung bestehender Modelle verarbeitet. Weiters sind viele dieser Modelle erst durch den Auf- und Ausbau des Internets möglich geworden.
   2. Da die automatisierte Datenverarbeitung in nahezu alle Bereiche des Berufs- und Privatlebens vordringt und immer mehr und schneller datenverarbeitende bzw. datenaustauschende Geräte mit immer höheren Speicherkapazitäten eingesetzt werden, wächst die Menge an verarbeiteten Daten in enormer Geschwindigkeit. Im Forschungsbereich wird proklamiert: „Ohne Daten keine Forschung!“
   3. Diese Umstände und (durch Technologiesprünge – Stichworte: „Künstliche Intelligenz“ oder „Quantencomputer“ – durchaus neue) Möglichkeiten führen einerseits zu immer mehr Bestrebungen zur Monetarisierung von Daten und andererseits zu (potentiellen) Missbräuchen im Zusammenhang mit Daten. Dementsprechend sind schon seit Längerem die (EU-)Gesetzgeber auf den Plan gerufen, die jeweils bestehende Rechtsordnung darauf zu prüfen, ob die Gesetze diesen neuen gesellschaftlichen Herausforderungen gewachsen sind. In vielen Bereichen sahen Gesetzgeber Handlungsbedarf und haben zahlreiche Normen verabschiedet bzw. zahlreiche Gesetzesinitiativen auf den Weg gebracht. Dennoch und zum Teil gerade wegen der neuen Rechtslage bestehen Rechtsunsicherheiten im Zusammenhang mit der Nutzung von Daten.
   4. Vor dem Hintergrund der
2. Notwendigkeit der Datenverarbeitung für Businessmodelle und/ oder
3. der Bestrebungen zur Monetarisierung von Daten

werden immer mehr Vereinbarungen rund um die Datennutzung geschlossen. Gegenständliche Einführung – und die darauf aufbauenden IPAG-Muster – sollen Hilfestellung zur Erstellung von entsprechenden Datennutzungsvereinbarungen liefern. Sämtliche Texte und Ausführungen beziehen sich auf die österreichische Rechtslage, doch versuchen die IPAG-Vertragsmuster zur Datennutzung möglichst unabhängig von der zugrundeliegenden Rechtsordnung einsetzbar zu sein, um auch für internationale Projekte herangezogen werden zu können. Allerdings stößt ein solches Bestreben gerade bei Daten rasch an seine Grenzen, weil die Rechtsnatur von Daten durchaus vielschichtig ist und die entsprechenden Rechtsrahmen nicht – nicht einmal in der EU – harmonisiert bzw. vereinheitlicht sind. Darüber hinaus fehlt es an entsprechender Rechtsprechung.

* 1. Ausgehend davon, dass praktisch nicht „Daten an sich“, sondern „Datenverkörperungen“ Gegenstand von Datennutzungsvereinbarungen sind, wird in der Folge zwar der Begriff „Daten“ verwendet, es sind damit aber durchwegs „Datenverkörperungen“ gemeint.

1. **Einstieg in die Rechtsnatur von Daten und Datennutzungsvereinbarungen**
   1. Folgende grafische Darstellung soll die wesentlichen Abgrenzungen der Rechtsnatur von Daten augenscheinlich machen (Details siehe unter 3 Weiterführendes Wissen), wobei diese Abgrenzungen auch für die jeweiligen Regelungsdimensionen einer Datennutzungsvereinbarung relevant und daher entsprechend abzubilden sind:

**Rechte des geistigen Eigentums**

**(IP)**

* 1. Es gilt daher bei Datennutzungsvereinbarungen von den Parteien insbesondere folgende Themen schon in der Planungsphase zu klären:
  2. Soweit personenbezogene Daten Gegenstand der Datennutzungsvereinbarung sind, ist auch von Beginn an mitzudenken, welche datenschutzrechtliche Rolle – also (getrennt oder gemeinsam) Verantwortlicher und/ oder Auftragsverarbeiter und/ oder Betroffener – die Vertragsparteien einnehmen, weil mit den Rollen jeweils unterschiedliche Pflichten und Rechte verbunden sind:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Der Betroffene ist derjenige, dessen personenbezogene Daten verarbeitet werden. Der Betroffene ist das primäre Schutzsubjekt des Datenschutzrechts (also insbesondere der DSGVO und des DSG), und er kann insbesondere seine Betroffenenrechte gegenüber dem Verantwortlichen (siehe gleich unten) geltend machen, also insbesondere das Recht auf Auskunft und u.U. Berichtigung, Löschung („Recht auf Vergessenwerden“), Datenübertragbarkeit und/oder Widerspruch.

Der sog „(datenschutzrechtliche) Verantwortliche“ ist der Hauptadressat der Pflichten des Datenschutzrechts. Verantwortlicher ist derjenige, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Er hat die „materielle und formelle Rechtmäßigkeit“ der Verarbeitung der personenbezogenen Daten sicherzustellen. Dabei hat er den Grundsatz zu beachten, dass es verboten ist, personenbezogene Daten zu verarbeiten, soweit kein gesetzlicher Rechtmäßigkeitsgrund die Verarbeitung erlaubt („materielle Rechtmäßigkeit“): Der Verantwortliche muss sich daher auf Rechtmäßigkeitsgründe für die Verarbeitung personenbezogener Daten stützen können, insbesondere eine gesetzliche Pflicht bzw. Ermächtigung zur Verarbeitung, die Erforderlichkeit zur Erfüllung eines Vertrags mit dem Betroffenen, berechtigte Interessen an der Verarbeitung und/ oder die Einwilligung des Betroffenen. Neben den Rechtmäßigkeitsgründen sind auch die gesetzlichen Gebote zur materiellen Rechtmäßigkeit einzuhalten, insbesondere das Zweckbindungs-, Datenminimierungs-, Richtigkeits-, Speicherdauerbegrenzungs-, Datensicherheits-, und Rechenschaftspflichtgebot. Die „formelle Rechtmäßigkeit“ betrifft insbesondere die ordnungsgemäße Datenschutzinformation, die Verzeichnisse der Verarbeitungstätigkeiten und den Abschluss von datenschutzgesetzlich verpflichtenden Vereinbarungen (Auftragsverarbeitervertrag bzw. Vertrag zwischen gemeinsam Verantwortlichen) und die Sicherstellung der Rechtmäßigkeit des etwaigen Internationalen Datentransfers über die Grenzen des EWRs hinaus.

Der Auftragsverarbeiter bzw. etwaige Sub-Auftragsverarbeiter sind diejenigen, welche ausschließlich im Auftrag des Verantwortlichen die personenbezogenen Daten des Betroffenen verarbeiten. Die primäre datenschutzgesetzliche Pflicht der Auftragsverarbeiter ist die Gewährleistung der Datensicherheit im Sinne der „technischen und organisatorischen (Schutz)Maßnahmen – TOMs“. Die Auftragsverarbeiter haben auch reduzierte Pflichten hinsichtlich der „formellen Rechtmäßigkeit“, nämlich bloß ein kleines Verarbeitungsverzeichnis und den Abschluss der datenschutzgesetzlich verpflichtenden Auftragsverarbeiterverträge.

Weiterführend zum Datenschutzrecht im Bereich von „Klinischen Studien“ siehe Punkt 7 - unten. Zu „Datenschutzrecht und Forschung“ siehe Punkt 8 unten.

* 1. Dementsprechend sollte möglichst früh von den Beteiligten folgende „Checkliste“ für Datennutzungsvereinbarungen abgearbeitet werden, um entsprechende Muster nutzen bzw. entsprechende Regelungen erstellen bzw. verhandeln zu können. Zu beachten ist dabei allerdings, dass manche Themen der Regelungskompetenz der Parteien entzogen sind, insbesondere:
* Sobald personenbezogene Daten an irgendeiner Stelle des Projekts verarbeitet werden, müssen die zwingenden Vorgaben des Datenschutzrechts beachtet werden. Soweit „sensible personenbezogene Daten“ – insbesondere personenbezogene Gesundheitsdaten – verarbeitet werden, gilt das noch strengere Regime der Verarbeitung besonderer Kategorien personenbezogener Daten.
* Auch die Rechte des geistigen Eigentums, insbesondere das Urheberrecht, sehen zwingende Regelungen vor, welche nicht oder nur unter besonderen Umständen durch Vereinbarungen abgeändert werden können, insbesondere der Bereich des Urheberpersönlichkeitsrechts, des (Vorab-)Verzichts auf gewisse Rechte nach dem Urheberrechtsgesetz usw.

1. **Weiterführendes Wissen**
   1. Trotz der Bestrebung, dass die IPAG-Vertragsmuster zur Datennutzung unabhängig von der Rechtsordnung eingesetzt werden können, ist – um den Regelungsbedarf in Datennutzungsverträgen vollständig erschließen zu können – das Wissen über eine Abgrenzung der Rechtsnatur von Daten erforderlich. Und wie so oft im juristischen Kontext, heißt es auch diesbezüglich: „es kommt darauf an!“. Darin, „worauf es ankommt“ – also in die unterschiedlichen rechtlichen Dimensionen von Daten – soll in der Folge eingeführt werden:
2. **Weiterführendes Wissen: Sachenrecht und „Dateneigentum“**
   1. Es ist zwischen
3. Daten – also (mündlicher bzw. im Arbeitsspeicher flüchtiger) Information an sich – und
4. „Datenverkörperungen“ – also (auf Papier) körperliche bzw. (auf einem physischen Datenträger) gespeicherte Datenbestände –

zu unterscheiden:

Ad (i): Bei Daten an sich kommen die sachenrechtlichen Regelungen – in Österreich, aber umso mehr in anderen Rechtsordnungen – an ihre rechtlichen bzw. rechtspraktischen Grenzen, sodass ein „Dateneigentum“ und die damit verbundenen gesetzlichen Regelungen wohl nicht anwendbar sind. Dennoch gehen die Autoren – trotz der grundsätzlich zwingenden und daher nicht der Parteiendisposition unterliegenden Regelungen des Sachenrechts – davon aus, dass zumindest zwischen den Vertragsparteien Regelungen vereinbart werden können, welche „dateneigentumsähnliche Wirkung“ entfalten. Allerdings wären diese vertraglichen Regelungen im Zweifel gegenüber nicht am Vertrag beteiligten Dritten, welche ja nicht Vertragspartei sind, unwirksam – genau dafür bräuchte es ein gesetzliches „Dateneigentum“. Nur mit einem Dateneigentum würde ein – auch gegenüber allen Dritten wirksames – absolutes Recht sichergestellt werden, sodass sich der Dateneigentümer auf die gesetzlichen Schutzvorschriften zugunsten von Eigentum berufen könnte, insbesondere zivilrechtliche Besitzstörungsklage, Eigentumsfreiheitsklage usw. Diese Instrumente können zwar vertraglich nachgebildet werden, gelten aber dann ausschließlich zwischen den Vertragsparteien.

Ad (ii): Bei Datenverkörperungen liegt hingegen die Qualifikation als „(körperliche) Sache“ im Sinne der (österreichischen) Gesetze nahe. Für die Qualifikation als körperliche Sache sind die objektiv feststellbare Existenz und die Beherrschbarkeit ausschlaggebend, wobei auch jeweils Mittelbarkeit – also durch Geräte – ausreicht. Damit könnten auf Datenverkörperungen sowohl die sachenrechtlichen als auch die schuldrechtlichen gesetzlichen Bestimmungen unmittelbar angewendet werden – also „echtes Eigentum an Datenverkörperungen“ bzw. „Daten(verkörperungs)eigentum“. Dann wäre es wohl möglich, nach den allgemeinen Regeln des Sachenrechts Eigentum an Datenverkörperungen zu erwerben, zu übertragen, aber auch zu verlieren. Der gesetzliche Besitz- und Eigentumsschutz wäre daher auch auf Datenverkörperungen anwendbar.

* 1. Ausgehend davon, dass Eigentum an Datenverkörperungen möglich ist, stellt sich die Frage, wie – neben dem abgeleiteten Eigentumserwerb durch Übertragung vom Voreigentümer – Eigentum an neu geschaffenen Datenverkörperungen entsteht. Dabei können folgende Fälle unterschieden werden:

1. Eigentumserwerb durch Schöpfung: der Schöpfer einer Datenverkörperung ist deren Eigentümer;
2. Eigentumserwerb durch Datenfruchtziehung: Datenverkörperungen, die durch andere Datenverkörperungen automatisiert generiert werden, stehen dem Fruchtgenussberechtigten (zumeist Eigentümer) der ursprünglichen Datenverkörperung zu;
3. Sonderfall zu (b) – durch Duplikation: da die Kopie inhaltlich ausschließlich vom Original bestimmt ist, ist das Eigentum an der Kopie dem Fruchtgenussberechtigten des Originals zuzuordnen.
   1. Über das neu geschaffene Eigentum an den Datenverkörperungen kann dann nach den allgemeinen sachenrechtlichen und schuldrechtlichen Regelungen verfügt werden.
   2. Die unten beschriebenen Bestimmungen des Immaterialgüterrechts und des Datenschutzrechts haben grundsätzlich keine Auswirkung auf die eigentumsrechtliche Zuordnung von Datenverkörperungen. Vielmehr regeln sie „nur“ zusätzliche – wenn auch nicht gänzlich entkoppelte (die Autoren sprechen daher von „Janusköpfigkeit“) – rechtliche Dimensionen an Daten(verkörperungen):
4. **Weiterführendes Wissen: „IP-Rechtliche Janusköpfigkeit von Daten(verkörperungen)“**
   1. Aufbauend auf dem lange strittigen, aber durch die Rechtsprechung in weiten Teilen geklärten Spannungsverhältnis zwischen Immaterialgüterrecht (insbesondere Urheberrecht, aber auch Marken-, Patenrecht udgl) und Sachen- bzw. Schuldrecht (insbesondere Gewährleistungsrecht) bei Computerprogrammen gehen die Autoren davon aus, dass eine „Janusköpfigkeit der Rechtsnatur der Daten(verkörperungen)“ besteht; mit anderen Worten: Daten(verkörperungen) können Regelungsgegenstand beider Rechtsbereiche sein, und wenn dies der Fall ist, müssen beide Regelungsbereiche beachtet und etwaige widersprüchliche Ergebnisse durch wechselseitige Beeinflussung der Auslegung der gesetzlichen Regelungen aufgelöst werden. Da es sich bei den meisten diesbezüglichen gesetzlichen Bestimmungen um dispositive Normen handelt, können die Parteien solche Widersprüche geringhalten, indem sie möglichst klare Vertragsbestimmungen hinsichtlich ihres Regelungswillens (auf Basis der gesetzlichen Möglichkeiten) festlegen. Im Zweifel wirken aber solche Regelungen nicht gegenüber Dritten, die nicht Partei der Vereinbarung wurden.
   2. Ähnlich der schon oben zum „Dateneigentum“ angesprochenen Unterscheidung zwischen unkörperlichen und körperlichen Sachen ist auch im Zusammenhang mit den Immaterialgüterrechten eine (gewisse) Verkörperung der Schutzgegenstände erforderlich. Bloße Ideen – also bloße Gedanken/Information – sind im Zweifel nicht durch Immaterialgüterrechte geschützt bzw. schützbar. Insoweit besteht ein gewisser Gleichlauf bei der „Janusköpfigkeit“ mit der Unterscheidung zwischen
5. Daten an sich und
6. Datenverkörperungen.

Es gilt dabei zu beachten, dass es sich beim Immaterialgüterrecht um spezialgesetzliche Bestimmungen handelt, welche praktisch wohl nur einen geringen Anwendungsbereich hinsichtlich Datenverkörperungen haben:

* 1. Für einen urheberrechtlichen Schutz bedürfte es bei der Datenverkörperung einer „eigentümlichen geistigen Schöpfung“ im Sinne des Urheberrechtsgesetzes. Für einen – ebenfalls im Urheberrechtsgesetz geregelten – Datenbankschutz müssten die in der Datenbank verkörperten Daten mit „nach Art oder Umfang wesentlichen Investitionen“ beschafft, überprüft oder dargestellt werden; ein mögliches aber jedenfalls nicht stets vorhandenes Kriterium für die gesetzliche Schutzfähigkeit.
  2. Für einen marken- bzw. patentrechtlichen Schutz müssten die Datenverkörperungen in den entsprechenden Registern eingetragen worden sein, wobei diesbezüglich gesetzliche Kriterien erforderlich und zum Teil von den Patent- bzw. Markenämtern von Amts wegen geprüft werden. Es ist daher zwar nicht auszuschließen, dass Datenverkörperungen auch Gegenstand dieser Immaterialgüterrechte sein können, doch kann dies nur äußerst einzelfallbezogen abgehandelt werden.
  3. Soweit klar bzw. nicht auszuschließen ist, dass Immaterialgüterrechte an den Datenverkörperungen bestehen (können), sollten die Datennutzungsvereinbarungen auch diese Dimension adressieren.

1. **Weiterführendes Wissen: „datenschutzrechtliche Janusköpfigkeit von Daten(verkörperungen)“**
   1. Hinsichtlich der datenschutzrechtlichen Dimension kann ebenfalls eine „Janusköpfigkeit“ von Daten(verkörperungen) gegeben sein. Auch diesbezüglich müssen dann beide Regelungsbereiche beachtet und etwaige widersprüchliche Ergebnisse durch wechselseitige Beeinflussung der Auslegung der Regelungen aufgelöst werden. Da die datenschutzrechtlichen Regelungen (als „Öffentliches Recht“) aber durchwegs der Parteiendisposition entzogen sind, können die Vertragsparteien nur beschränkt Widersprüche durch vertragliche Regelungen auflösen. Mit anderen Worten: Aufgrund des zwingenden Charakters gehen im Fall widersprüchlicher Ergebnisse die Regelungen des Datenschutzrechts den Regelungen zum Eigentum bzw. auch zum Immaterialgüterrecht vor.
   2. Hinsichtlich der möglichen datenschutzrechtlichen Dimension bei Datennutzungsvereinbarungen sind drei Szenarien streng voneinander zu unterscheiden:
2. auf „anonyme Daten“ ist das Datenschutzrecht nicht anwendbar, sodass die datenschutzrechtliche Dimension unbeachtet bleiben kann;
3. bei „personenbezogenen Daten“ – einschließlich „pseudonymisierter Daten“ – ist das Datenschutzrecht anwendbar;
4. bei „sensiblen Daten“ gelten besondere datenschutzrechtliche Anforderungen:
   1. Ad (i) - anonyme Daten: Diese sind im Datenschutzrecht nicht definiert. Ihre Abgrenzung erschließt sich aus dem Umkehrschluss der Legaldefinition von „personenbezogenen Daten“; mit anderen Worten: Daten, die nicht personenbezogen sind, sind anonyme Daten. 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 (ErwG 26 der DSGVO). Hinsichtlich der Dimension der „Identifizierbarkeit“ besteht ein „bewegliches System“, weil dabei alle Mittel berücksichtigt werden müssen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Person direkt oder indirekt zu identifizieren. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollen alle objektiven Faktoren herangezogen werden: insbesondere die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand. Dafür sind die zum Zeitpunkt der Verarbeitung verfügbare Technologie sowie technologische Entwicklungen zu berücksichtigen. Ein Anonymisierungsverfahren verhindert – zumindest im datenschutzrechtlichen Umfeld – dann in angemessener Weise eine Re-Identifikation, wenn sie für drei Risiken, nämlich

(a) Aussonderung („singling out“),

(b) Verlinkbarkeit („linkability“) und

1. Rückschluss („inference“) eine Lösung bietet.

Dabei ist in einer *ex ante*-Betrachtung darauf abzustellen, wie hoch nach allgemeinem Ermessen die Wahrscheinlichkeit ist, dass in den konkreten Datenbeständen in einer *ex post*-Betrachtung ein Personenbezug hergestellt wird. Hierfür sind folgende Beurteilungsdimensionen – im Sinne eines „beweglichen Beurteilung-Systems“ – heranzuziehen:

(aa) Mittel, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um Personenbezug herzustellen und dabei:

1. Art, Umfang, Umstände und Zwecke der Verarbeitung;
2. Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen;
3. Kosten der Identifizierung; und
4. erforderlicher Zeitaufwand,
5. wobei jeweils die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Soweit (bb) man dabei zu dem Schluss kommt, dass ohne unverhältnismäßigen Aufwand eine Wiederherstellung des Personenbezugs nicht erwartbar ist, liegen anonyme Daten vor.

Liegen durchgehend anonyme Daten im Rahmen der Durchführung einer Datennutzungsvereinbarung vor, ist – mit Ausnahme einer Garantie aller Parteien, jedenfalls keinen Personenbezug herzustellen – die datenschutzrechtliche Dimension nicht weiter zu beachten.

* 1. Ad (ii) - personenbezogene Daten: Das Datenschutzrecht definiert „personenbezogene Daten“ denkbar weit als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“ (Art 4 Z 1 DSGVO).

Die Qualifikation als personenbezogenes Datum hat deswegen eine so hohe praktische Relevanz, weil im Datenschutzrecht der „Verbotsgrundsatz mit Erlaubnisvorbehalt“ gilt; mit anderen Worten: Es ist grundsätzlich verboten, personenbezogene Daten zu verarbeiten, außer der Verarbeitende kann sich auf einen datenschutzgesetzlichen Rechtmäßigkeitsgrund stützen („materielle Rechtmäßigkeit“) und hält auch die datenschutzgesetzlichen Rahmenbedingungen, wie insbesondere Datensicherheit, Betroffenenrechte, Verfahrensverzeichnis, datenschutzrechtliche Vereinbarungen udgl, ein („formelle Rechtmäßigkeit“).

Die materielle und formelle Rechtmäßigkeit der Verarbeitung personenbezogener Daten leitet sich aus den Grundsätzen (Art 5 DSGVO – von den Autoren „datenschutzrechtliche Gebote“ genannt) ab: demnach müssen für eine rechtmäßige Verarbeitung die personenbezogenen Daten

(a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Gebote der "Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz").

Zum Rechtmäßigkeitsgebot siehe unten im Detail die Rechtmäßigkeitsgründe (Art 6 DSGVO und für „sensible Daten“ Art 9 DSGVO).

(b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Gebot der "Zweckbindung").

Das Zweckbindungsgebot darf aber nicht übertrieben streng verstanden werden (vgl auch Art 6 Abs 4 DSGVO). So kann zum Beispiel die Errichtung einer Testdatenbank parallel zu einer anderen Datenbank noch vom Zweckbindungsgrundsatz und den berechtigten Interessen gedeckt sein (EuGH C-77/21), sodass diesbezüglich bei Datennutzungsvereinbarungen durchaus „Bewegungsspielraum“ gegeben ist.

(c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Gebot der "Datenminimierung").

(d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Gebot der "Richtigkeit").

(e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Gebot der "Speicherbegrenzung").

(f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (Gebote der "Integrität und Vertraulichkeit").

wobei (g) die Einhaltung von (a) bis (f) nachgewiesen werden können muss ("Rechenschaftspflicht").

Zum Rechtmäßigkeitsgebot: Die Verarbeitung von personenbezogenen Daten ist ausschließlich auf Basis zumindest eines der folgenden Rechtmäßigkeitsgründe möglich, wobei diese im Gesetz zum Teil näher ausgestaltet werden (siehe im Detail Art 6 DSGVO): (aa) Einwilligung für einen oder mehrere bestimmte Zwecke (vgl für die Anforderungen an eine rechtmäßige Einwilligung auch Art 7 f DSGVO); (bb) Erforderlichkeit für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen; (cc) Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung; (dd) Erforderlichkeit, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; (ee) Erforderlichkeit zur

Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde; (ff) Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen der betroffenen Person überwiegen (dieser Rechtmäßigkeitsgrund gilt nicht für Behörden in Erfüllung ihrer Aufgaben).

* 1. Ad (iii) – „sensible Daten“: Auf diese besonders schutzwürdige Kategorie von personenbezogenen Daten sind (noch) strengere Regelungen des Datenschutzrechts anwendbar. Dabei ist zu beachten, dass eine abschließende Liste von „sensiblen Daten“ definiert ist, nämlich personenbezogene Daten, aus denen (a) die rassische und ethnische Herkunft, (b) politische Meinungen, (c) religiöse oder weltanschauliche Überzeugungen oder (d) die Gewerkschaftszugehörigkeit hervorgehen, sowie (e) genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, (f) Gesundheitsdaten oder (g) Daten zum Sexualleben oder der sexuellen Orientierung (Art 9 DSGVO). Ad (f) – Gesundheitsdaten werden definiert als personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art 4 Z 15 DSGVO).

Bei Datennutzungsvereinbarungen ist außerdem zu beachten, dass ein durchaus breites Verständnis von „sensiblen Daten“ anzuwenden ist, weil zum Beispiel auch „indirekt sensible Informationen“ unter das strenge Regime fallen (EuGH C-184/20).

Die Verarbeitung von „sensiblen Daten“ ist ausschließlich auf Basis folgender Rechtmäßigkeitsgründe möglich, wobei diese im Gesetz zum Teil näher ausgestaltet werden (vgl im Detail Art 9 DSGVO):

(aa) ausdrückliche Einwilligung;

(bb) Erforderlichkeit nach dem Arbeitsrecht;

(cc) Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben;

(dd) Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisation;

(ee) die Verarbeitung bezieht sich auf personenbezogene Daten, welche die betroffene Person offensichtlich öffentlich gemacht hat;

(ff) Durchsetzung von Rechtsansprüchen;

(gg) gesetzliche Ermächtigung;

(hh) Erforderlichkeit für Zwecke der Gesundheitsvorsorge durch ein einem Berufsgeheimnis unterliegenden Fachpersonal;

(ii) Erforderlichkeit im Bereich der öffentlichen Gesundheit; und/ oder

(jj) Erforderlichkeit für (gesetzliche) Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

Unter Umständen sind bei Datennutzungsvereinbarungen neben obgenannten materiellrechtlichen Anforderungen für eine rechtmäßige Verarbeitung von „sensiblen Daten“ auch erhöhte Datensicherheitsmaßnahmen zu ergreifen (vgl Art 32 DSGVO).

Wenn auch nicht formell unter „sensible Daten“ fallend, unterliegt die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (diese Begriffe sind sehr weit zu verstehen) besonderen Beschränkungen (Art 10 DSGVO): Grundsätzlich darf die Verarbeitung nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach einer entsprechenden gesetzlichen Ermächtigung zulässig ist (vgl idZ § 4 Abs 3 DSG). Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

* 1. Zentraler Normadressat des Datenschutzrechts ist der sogenannte „Verantwortliche“, also derjenige, welcher über Zwecke und Mittel der Verarbeitung entscheidet (Art 4 Z 7 DSGVO). Der Verantwortliche hat die Rechtmäßigkeit der gesamten Datenverarbeitung sowohl in „materieller“ (Rechtmäßigkeit ieS) als auch in „formeller“ Hinsicht (Einhaltung der datenschutzgesetzlichen „Formalvoraussetzungen“, wie Gewährung der Betroffenenrechte, insbesondere Datenschutzinformation, Datensicherheit in der gesamten Verarbeitungskette, großes Verfahrensverzeichnis udgl) sicherzustellen.
  2. Davon abzugrenzen ist der „Auftragsverarbeiter“, welcher personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art 4 Z 8 DSGVO). Den Auftragsverarbeiter treffen grundsätzlich keine „materiellen Pflichten“ (er hat sich in der Regel nicht um die Rechtmäßigkeit ieS zu kümmern), und ihn treffen nur eingeschränkte „formelle Pflichten“ (Datensicherheit in seinem Bereich, kleines Verfahrensverzeichnis udgl).
  3. Schutzsubjekt des Datenschutzrechts ist der Betroffene, also derjenige, dessen personenbezogene Daten verarbeitet werden (vgl Art 4 Z 1 DSGVO).

1. **Weiterführendes Wissen: Daten und Klinische Studien**
   1. Mit sog. „klinischen Studien“ zu Arzneimitteln (siehe Definition in § 2a AMG) gehen zwingend die Generierung und in weiterer Folge die Verarbeitung von personenbezogenen Gesundheitsdaten der Probanden bzw. der Patienten („Prüfungsteilnehmer“) einher. Gemäß § 41 AMG muss der Prüfungsteilnehmer, oder, falls dieser nicht entscheidungsfähig ist, sein gesetzlicher Vertreter, schriftlich und ausdrücklich über Zweck und Umfang der Erhebung und Verarbeitung personenbezogener Daten (also unter Umständen nicht nur jene des Prüfungsteilnehmers) aufgeklärt werden und in die Datenverarbeitung einwilligen. Somit sind die Voraussetzungen der Einwilligung in klinische Studien strenger als die Voraussetzungen nach den allgemeinen datenschutzrechtlichen Vorschriften (insb Artt 7 und 9 DSGVO). § 41 Abs 3 AMG regelt auch die Verarbeitung im Sonderfall des Todes des Prüfungsteilnehmers bzw. Endes der Prüfung nach Aufklärung des Prüfungsteilnehmers aber vor dessen Abgabe der Einwilligung.
   2. Andererseits ist diese AMG-Einwilligung ein breiterer Rechtmäßigkeitsgrund als die allgemeine Einwilligung: Der Widerruf der AMG-Einwilligung durch den Prüfungsteilnehmer hat nämlich keine Auswirkungen auf „Tätigkeiten“, die auf der Grundlage der AMG-Einwilligung vor dem Widerruf durchgeführt wurden, und auch nicht auf die Verarbeitung der auf dieser Grundlage erhobenen Daten (§ 41 Abs 2 AMG).
   3. Das AMG schließt das Recht auf Löschung („Recht auf Vergessenwerden“ – Art 17 DSGVO) und das Recht auf Datenübertragbarkeit (Art 20 DSGVO) aus. Darüber ist allerdings im Zuge der Aufklärung zur Einholung der Einwilligung explizit hinzuweisen (§ 41 Abs 2 AMG).
   4. Wie bei jeder datenschutzrechtlichen Beurteilung ist es auch bei klinischen Studien äußerst relevant, die datenschutzrechtlichen Rollen als Verantwortlicher bzw. als Auftragsverarbeiter korrekt zuzuweisen, um den datenschutzrechtlichen Pflichten (auch nach dem AMG) gerecht werden zu können. Die drei Hauptakteure bei klinischen Studien sind (i) die Prüfpersonen (Probanden bzw. Patienten als datenschutzrechtlicher Betroffener), der Sponsor (meist das pharmazeutische Unternehmen) und der Prüfer (der studiendurchführende Arzt). Die datenschutzrechtliche Rollenverteilung zwischen Sponsor und Prüfer wird im AMG nicht geregelt, sodass diese nach den allgemeinen datenschutzrechtlichen Maßstäben – unter Umständen unterschiedlich je Verarbeitungsschritt – zu ermitteln ist:
   5. Dementsprechend ist im Einzelfall je konkreter Ausgestaltung der Entscheidung über Zwecke und Mittel der Datenverarbeitung zu prüfen, ob und wann getrennte Verantwortlichkeit, gemeinsame Verantwortlichkeit (Art 26 DSGVO), oder in Ausnahmefällen sogar eine Auftragsverarbeitung (Art 28 DSGVO) vorliegt. Aufgrund des unmittelbaren Kontaktes, der Aufklärungspflicht und der unmittelbaren Erhebung der Daten des Prüfungsteilnehmers durch den Prüfer ist dieser in der Regel derjenige, welcher (zumindest diesbezüglich – vgl auch § 43 Abs 4 Z 1 und 2 AMG) über Zweck und Mittel der Datenverarbeitung; je detaillierter der Sponsor diese Zwecke und Mittel (mit)bestimmt, desto eher liegt gemeinsame Verantwortlichkeit vor. In weiterer Folge wird in der Regel getrennte Verantwortlichkeit vorliegen, weil der Sponsor dann mit den an ihn übermittelten (pseudonymisierten) Daten eigene Zwecke und Mittel verfolgt. Dementsprechend haben Prüfer und Sponsor die genauen Umstände der Verarbeitungsschritte zu definieren, um die entsprechenden datenschutzrechtlichen Rollen zuzuteilen. § 43 Abs 4 AMG bestimmt in diesem Zusammenhang – sodass die Vereinbarungen zwischen Prüfer und Sponsor an diesen „Leitplanken“ zu erfolgen hat –, dass es die Aufgabe des Prüfers ist, (i) die Daten korrekt zu verarbeiten, insbesondere zu erheben, zu erfassen und zu übermitteln; (ii) die Daten ehestmöglich zu pseudonymisieren, die Pseudonymisierung zu dokumentieren, die Dokumentation mit äußerster Sorgfalt handzuhaben und sicherzustellen, dass die Zuordnung zu einer spezifischen betroffenen Person (= Prüfungsteilnehmer) ausschließlich unter den im Prüfplan angegebenen Umständen erfolgt; (iii) für den Sponsor die (verbleibenden) Pflichten nach den Betroffenenrechten (Artt 13, 15, 16 und 18 DSGVO) zu erfüllen, und (iv) bei Verletzungen des Schutzes personenbezogener Daten den Prüfungsteilnehmer zu benachrichtigen (vgl Art 34 DSGVO) und den Sponsor davon zu informieren.
   6. Unabhängig von obigen Rollenverteilungen verweist das AMG für eine etwaige Weiterverarbeitung der Daten, welche im Rahmen der klinischen Studie erhoben bzw. verarbeitet wurden, auf § 2d Abs 3 des ForschungsorganisationsG (FOG) - siehe dazu unten.
   7. Der Vollständigkeit halber: Obiges gilt – mit Ausnahme des Sonderfalls des Todes des Prüfungsteilnehmers – auch für nichtinterventionelle Studien.
2. **Weiterführendes Wissen: Datenschutzrecht und Forschung** 
   1. Der grundsätzlich unmittelbar anwendbare europäische Datenschutzrechtsrahmen (DSGVO) sieht in gewissen Bereichen sog. „Öffnungsklauseln“ vor, die den Gesetzgebern der Mitgliedsstaaten Spielräume für nationale Bestimmungen einräumen. In Durchführung des Art 9 Abs 2 lit j DSGVO sowie des Art 89 DSGVO ergingen in Österreich § 7 DSG (der inhaltlich weitgehend dem alten § 46 DSG 2000 entspricht) sowie das ForschungsorganisationsG (FOG). Nach den erläuternden Bemerkungen des Gesetzgebers soll das FOG den Regelungen des § 7 DSG vorgehen, sodass Letztgenannter im Forschungsbereich wohl de facto unanwendbar ist; daher wird in der Folge ausschließlich auf das FOG eingegangen.
   2. Das FOG sieht umfassende – unter Umständen sogar europarechtswidrig zu weit gehende – Privilegien bzw. Vereinfachungen des datenschutzrechtlichen Rahmens der Verarbeitung von personenbezogenen Daten für wissenschaftliche Einrichtungen vor. Diese sind durchaus breit definiert, nämlich als „natürliche Personen, Personengemeinschaften sowie juristische Personen, die [Forschungs]Zwecke […] verfolgen, d.h. insbesondere Tätigkeiten der Forschung und experimentellen Entwicklung […] vornehmen, ungeachtet dessen, ob dies (a) zu gemeinnützigen Zwecken (§§ 34 ff der Bundesabgabenordnung) oder nicht oder (b) im universitären, betrieblichen oder außeruniversitären Rahmen erfolgt“.
   3. Das FOG normiert somit weitreichende Erlaubnistatbestände, deren Voraussetzungen teilweise sehr abstrakt formuliert sind. Durch den „Grundtatbestand“ (§ 2d Abs 2 Z 1 FOG) wurden im Forschungsbereich pauschal (fast) alle Datenverarbeitungsmethoden erlaubt, unter der einzigen Bedingung, dass der Verantwortliche bestimmte „Datensicherheitsmaßnahmen“ einhält: Für Forschungszwecke dürfen wissenschaftliche Einrichtungen (siehe breite Definition oben), sämtliche personenbezogenen Daten jedenfalls verarbeiten, insbesondere im Rahmen von Big Data, personalisierter Medizin, biomedizinischer Forschung, Biobanken und der Übermittlung an andere wissenschaftliche Einrichtungen und Auftragsverarbeiter, wenn (a) anstelle des Namens bereichsspezifische Personenkennzeichen oder andere eindeutige Identifikatoren zur Zuordnung herangezogen werden oder (b) die Verarbeitung in pseudonymisierter Form erfolgt oder (c) Veröffentlichungen (aa) nicht oder (bb) nur in anonymisierter oder pseudonymisierter Form erfolgen oder (d) die Verarbeitung ausschließlich zum Zweck der Anonymisierung oder Pseudonymisierung erfolgt und keine Offenlegung direkt personenbezogener Daten an Dritte damit verbunden ist.
   4. Weiter privilegiert das FOG die sog. „Registerforschung“: Wissenschaftliche Einrichtungen (und auch Inhaber einer gültigen Bestätigung gemäß § 2c Abs 2 FOG) dürfen von Verantwortlichen, die bundesgesetzlich vorgesehene Register – mit Ausnahme der in den Bereichen der Gerichtsbarkeit sowie der Rechtsanwälte und Notare im Rahmen des jeweiligen gesetzlichen Wirkungsbereichs geführten Register und des Strafregisters – führen, sowie im Falle von ELGA von der ELGA-Ombudsstelle, den Zugang zu Daten, bei denen keine Identifizierung von betroffenen Personen oder Unternehmen durch Namen, Anschrift oder anhand einer öffentlich zugänglichen Identifikationsnummer möglich ist, aus diesen Registern in elektronischer Form verlangen, wenn (a) die Verarbeitung (aa) ausschließlich für Zwecke der Lebens- und Sozialwissenschaften erfolgt und (bb) auch einem öffentlichen Interesse dient, (b) das Register in einer Verordnung des Wissenschaftsministers angeführt ist, (c) die Kosten für die Gewährung des Zugangs zu Daten ersetzt werden und (e) falls ein Abgleich mit vorhandenen Daten beantragt wird, beim Antrag auf Gewährung des Zugangs zu Daten die entsprechenden bPK der betroffenen Personen zur Verfügung gestellt werden.
   5. Weiters dürfen wissenschaftliche Einrichtungen Forschungsmaterial (§ 2b Z 6 FOG) für Forschungszwecke insbesondere sammeln, archivieren und systematisch erfassen und dazu sämtliche Daten verarbeiten, die erforderlich sind, um einen optimalen Zugang zu Daten und Forschungsmaterial für „Register“-Zwecke zu gewährleisten (siehe Details in § 2f Abs 1 und 2 FOG).
   6. Darüber hinaus dürfen Daten und Forschungsmaterial, die als Grundlage für Tätigkeiten zu Forschungszwecken verarbeitet wurden („Rohdaten“), ab Veröffentlichung der Ergebnisse dieser Tätigkeiten (i) zum Nachweis der Einhaltung guter wissenschaftlicher Praxis mindestens zehn Jahre sowie (ii) zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen bis zu 30 Jahre verarbeitet werden (§ 2f Abs 3 FOG).
   7. Die Verarbeitungen im Rahmen von biologischen Proben- und Datensammlungen aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, stellen zulässige Verarbeitungen dar. Die Verantwortlichen haben jedenfalls die folgenden angemessenen und spezifischen Maßnahmen vorzusehen: (i) die schnellstmögliche Pseudonymisierung, wenn dennoch die Zwecke der Verarbeitungen erfüllt werden können, sowie (ii) die Einhaltung der erforderlichen Datensicherheitsmaßnahmen.
   8. Für Zwecke der Lehre, insbesondere das Verfassen schriftlicher Seminar- und Prüfungsarbeiten, Bachelorarbeiten sowie wissenschaftlicher und künstlerischer Arbeiten durch Studierende, dürfen sämtliche personenbezogenen Daten verarbeitet werden, wenn sichergestellt ist, dass – außer zulässigen Verarbeitungen – keine Übermittlung an Empfänger zu anderen Zwecken erfolgt.
   9. Für Zwecke der medizinischen Forschung und sterbefallbezogener Analysen darf die Bundesanstalt Statistik Österreich wissenschaftlichen Einrichtungen nach Vereinbarung der konkreten Anwendungsbereiche und eines angemessenen Kostenersatzes das Sterbedatum und die Todesursache von Betroffenen übermitteln. Die wissenschaftlichen Einrichtungen und deren Angehörige unterliegen hinsichtlich dieser Daten der Geheimhaltungspflicht gemäß Bundesstatistikgesetz und dürfen diese Daten ausschließlich für wissenschaftliche Zwecke verwenden. An Medizinischen Universitäten bzw. Universitäten, an denen eine Medizinische Fakultät eingerichtet ist, ist vor Übermittlung die Ethikkommission gemäß § 30 UG zu befassen. An anderen wissenschaftlichen Einrichtungen ist – sofern vorhanden – eine Ethikkommission gemäß § 8c KAKuG oder eine vergleichbare Ethikkommission zu befassen.
   10. Darüber hinaus ist die Bildverarbeitung für wissenschaftliche Zwecke im Bereich des § 44 KAKuG privilegiert: Sowohl der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten als auch die Auswertung von mittels Bildaufnahmen gewonnen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art 9 DSGVO) als Auswahlkriterium für Forschungszwecke sind zulässig, vorausgesetzt (i) die Verarbeitung erfolgt durch wissenschaftliche Einrichtungen und (ii) durch die Verarbeitung erfolgt keine Veröffentlichung personenbezogener Daten.
   11. Soweit obige Privilegien nicht ohnehin schon greifen, dürfen nach § 2d Abs 3 in Forschungsbereich personenbezogene Daten verarbeitet werden, wenn die betroffene Person freiwillig, in informierter Weise und unmissverständlich ihren Willen in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung bekundet, mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden zu sein, wobei die Angabe eines Zweckes durch die Angabe (i) eines Forschungsbereiches oder (ii) mehrerer Forschungsbereiche oder (iii) von Forschungsprojekten oder (iv) von Teilen von Forschungsprojekten erfolgen darf („broad consent“).
   12. Gemäß § 2h FOG dürfen wissenschaftliche Einrichtungen (i) wissenschaftliche Mitarbeiter, die sich in einem aufrechten Arbeitsverhältnis zur jeweiligen wissenschaftlichen Einrichtung befinden, namentlich mit Foto und einer Liste ihrer Publikationen (a) auf einer Website der wissenschaftlichen Einrichtung oder (b) im Rahmen öffentlich zugänglicher Berichte der wissenschaftlichen Einrichtung anführen, es sei denn, die Veröffentlichung ist geeignet, die öffentliche Sicherheit, die Strafrechtspflege, die umfassende Landesverteidigung, die auswärtigen Beziehungen oder ein berechtigtes privates oder geschäftliches Interesse zu verletzen, wobei der Veröffentlichung eines Fotos gemäß (a) jederzeit widersprochen werden kann, oder (ii) wissenschaftliche Mitarbeiter, die sich nicht mehr in einem aufrechten Arbeitsverhältnis zur jeweiligen wissenschaftlichen Einrichtung befinden, sowie Studierende namentlich (a) auf einer Website der wissenschaftlichen Einrichtung oder (b) im Rahmen öffentlich zugänglicher Berichte der wissenschaftlichen Einrichtung anführen, es sei denn, die Veröffentlichung ist geeignet, die öffentliche Sicherheit, die Strafrechtspflege, die umfassende Landesverteidigung, die auswärtigen Beziehungen oder ein berechtigtes privates oder geschäftliches Interesse zu verletzen, oder (iii) insbesondere auch folgende Daten von ehemaligen wissenschaftlichen Mitarbeitern sowie von ehemaligen Studierenden verarbeiten und mit anderen öffentlich zugänglichen Informationen verknüpfen: (a) Forschungsschwerpunkte sowie (b) Angaben zu Publikationen, oder (iv) Angaben zu natürlichen Personen, wie insbesondere (a) Namensangaben, (b) Personenmerkmale sowie (c) Angaben zum Lebenslauf von Wissenschaftlern sowie ihnen nahestehenden Personen verarbeiten.
   13. Wissenstransfer ist unter den Voraussetzungen des „Grundtatbestands“ (siehe oben) zulässig. § 2i FOG normiert eine Privilegierung für den Wissens- und Technologietransfer: Ungeachtet allfälliger patentrechtlicher Bestimmungen ist die Verarbeitung, insbesondere Übermittlung personenbezogener Daten, für Technologietransfer zulässig, wenn (i) diese Verarbeitung erforderlich ist, um die Funktionalität der zu transferierenden Technologie zu erhalten, und (ii) insbesondere durch Technikgestaltung sichergestellt ist, dass Dritte keine tatsächliche Kenntnis der übermittelten Daten erlangen. Dann finden die Betroffenenrechte (Art 12 bis 22 DSGOV) und Data Breach Notification-Pflichten (Art 34 DSGVO) keine Anwendung.
   14. Werden im Rahmen von Open-Science- und Citizen-Science-Projekten eigene personenbezogene Daten freiwillig zur Verfügung gestellt, ist ihre Verarbeitung für die zu Beginn des Projekts ausdrücklich kommunizierte Art, Umfang und Dauer zulässig (§ 2i Abs 4 FOG). Die Löschung ist nur zulässig, wenn dadurch (i) die Projektziele und (ii) die methodischen, insbesondere statistischen, Anforderungen an wissenschaftliches Arbeiten nicht beeinträchtigt werden. Werden im Rahmen von Open-Science- und Citizen-Science-Projekten personenbezogene Daten Dritter zur Verfügung gestellt, ist ihre Verarbeitung für die zu Beginn des Projekts ausdrücklich kommunizierte Art, Umfang und Dauer jedenfalls zulässig, wenn (i) die Daten auf Beobachtungen oder Messungen im öffentlichen Raum beruhen oder (ii) die Daten pseudonymisiert werden. Die Löschung ist nur unter obigen Voraussetzungen zulässig.
   15. Schließlich ist die „Internationalität von Verarbeitungen zu Forschungszwecken“ privilegiert (§ 2j FOG): Übermittlungen an (a) wissenschaftliche Einrichtungen, (b) Förder- und Zuwendungsstellen, (c) Gutachter, (d) österreichische öffentliche Stellen (§ 2b Z 8 FOG) und Wissens- und Technologietransfer in Mitgliedstaaten der Europäischen Union sind zulässig.
   16. Neben obgenannten Privilegien hinsichtlich der materiellen Rechtmäßigkeit bestehen nach dem FOG auch Privilegien hinsichtlich der formellen Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im Forschungsbereich:
3. Personenbezogene Daten dürfen für diese Zwecke unbeschränkt gespeichert und gegebenenfalls sonst verarbeitet werden, soweit gesetzlich keine zeitlichen Begrenzungen vorgesehen sind (§ 2d Abs 5 FOG).
4. Die folgenden Betroffenenrechte finden im Forschungsbereich keine Anwendung, wenn dadurch die Erreichung der Forschungszwecke voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtigt wird: (a) Auskunftsrecht der betroffenen Person (Art. 15 DSGVO), (b) Recht auf Berichtigung (Art. 16 DSGVO), (c) Recht auf Löschung bzw. Recht auf Vergessenwerden (Art. 17 DSGVO), (d) Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), (e) Recht auf Datenübertragbarkeit (Art. 20 DSGVO) sowie (f) Widerspruchsrecht (Art. 21 DSGVO).
   1. Neben den Privilegierungen sind allerdings auch ergänzende Pflichten nach dem FOG zu erfüllen, insbesondere
5. über automationsunterstützte Verarbeitungen von personenbezogenen Daten ist Protokoll zu führen, damit tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können;
6. Verantwortliche und Auftragsverarbeiter, die personenbezogene Daten auf Grundlage dieses Abschnitts verarbeiten und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten, die ihnen anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis);
7. natürliche Personen, deren personenbezogene Daten auf Grundlage des FOG verarbeitet werden, dürfen keine Nachteile aus der Verarbeitung erleiden, wobei die Verarbeitung in Übereinstimmung mit dem FOG keinen Nachteil darstellt.
8. Verantwortliche, welche die Verarbeitungen auf das FOG stützen, haben:
9. im Internet öffentlich einsehbar auf die Inanspruchnahme dieser Rechtsgrundlage hinzuweisen,
10. bei Ausstattung ihrer Daten mit bereichsspezifischen Personenkennzeichen die Namensangaben sowie andere Personenkennzeichen (abgesehen von den bereichsspezifischen Personenkennzeichen „Forschung“ (bPK-BF-FO) und bereichsspezifischen Personenkennzeichen in verschlüsselter Form (vbPK)) jedenfalls zu löschen,
11. vor Heranziehung von Registern (siehe oben zur „Registerforschung“) einen Datenschutzbeauftragten (vgl Art 37 DSGVO) zu bestellen,
12. die Aufgabenverteilung bei der Verarbeitung der Daten zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
13. die Verarbeitung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
14. jeden Mitarbeiter über seine datenschutzrechtlichen Pflichten einschließlich der Datensicherheitsvorschriften zu belehren,
15. die Zutrittsberechtigung zu den Räumlichkeiten, in denen die Verarbeitung der Daten erfolgt, zu regeln,
16. die Zugriffsberechtigung auf Daten und Programme und den Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
17. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
18. eine Dokumentation über die nach (d) bis (i) getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern,
19. bei „Registerforschung“ (siehe oben) in ihrem Antrag auf Zugang zu Daten anzugeben:

(aa) die Gründe, warum das Forschungsvorhaben nur mittels des vorgesehenen Zugangs durchgeführt werden kann,

(bb) die natürlichen Personen, die Zugang zu Daten erhalten sollen,

(cc) die Datensätze, zu denen Zugang benötigt wird, und die Methoden ihrer Analyse sowie

(dd) die angestrebten Ergebnisse des Forschungsvorhabens,

1. bei „Registerforschung“ vorzusehen, dass nur die im Antrag genannten natürlichen Personen auf diese Daten zugreifen dürfen.
2. bei „Registerforschung“ bei Übermittlung von Namensangaben diese nach Erreichung der Zwecke zu löschen.
   1. Zu den Details der bereichsspezifischen Personenkennzeichen für den Tätigkeitsbereich „Forschung“ (bPK-BF-FO) siehe §§ 2c und 2d Abs 2 (insb Z 2) und Abs 9 FOG. Die Veröffentlichung von Personenkennzeichen darf unter keinen Umständen erfolgen (§ 2d Abs 1 Z 6 FOG).
   2. Das FOG sieht auch Privilegien hinsichtlich Strafen und anderer Rechtsfolgen bei Verstößen gegen das Datenschutzrecht vor: allgemein sind solche Konsequenzen aufgrund von § 30 Abs 5 DSG für Behörden und öffentliche Stellen ausgeschlossen. Durch § 2k Abs 2 Z 12 FOG wurde der Kreis der Privilegierten auf Auftragsverarbeiter von Behörden und öffentlichen Stellen erweitert.