

# Art. 26 DS-GVO: Gemeinsam Verantwortliche

---

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und  
Epidemiologie e. V.



Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Version 1.0

Stand: 17. 06. 2018

## **Autoren**

Bernd Schütze  
Gerald Spyra

Deutsche Telekom Healthcare and Security GmbH  
Ratajczak und Partner mbB Rechtsanwälte

## Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

## Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:



- Teilen: Das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: Das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen, solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

<https://creativecommons.org/licenses/by-sa/4.0/deed.de>

bzw. für den vollständigen Lizenztext

<https://creativecommons.org/licenses/by-sa/4.0/legalcode>

# Inhaltsverzeichnis

<b>Art. 26 DS-GVO: Gemeinsam Verantwortliche</b>	<b>1</b>
<b>Zusammenfassung</b>	<b>3</b>
<b>1 Einleitung</b>	<b>4</b>
<b>2 Erläuterungen zum rechtlichen Hintergrund</b>	<b>5</b>
2.1 Definition „gemeinsam Verantwortliche“	5
2.1.1 Abgrenzung zur Auftragsverarbeitung	5
2.1.2 Beispiele	6
2.2 Erlaubnistatbestand	7
2.3 Vereinbarung zwischen gemeinsam Verantwortlichen	7
2.4 Information betroffener Personen	8
2.5 Rechte der betroffenen Person	9
2.6 Beschränkung	9
2.7 Zuständige Aufsichtsbehörde	9
2.8 Haftung	9
2.9 Sanktionierung	10
<b>3 Checklisten: Was vorab zu prüfen ist</b>	<b>11</b>
3.1 Allgemeine Fragen	11
3.2 Abgrenzung Verantwortlichkeiten / Beteiligung an der Verarbeitung	12
<b>4 Abkürzungen</b>	<b>13</b>
<b>5 Literatur</b>	<b>14</b>
5.1 Online	14
5.2 Zeitschriften	14
<b>Muster-Vereinbarung</b>	<b>15</b>
<b>Präambel</b>	<b>15</b>
<b>§ 1: Definitionen</b>	<b>15</b>
<b>§ 2: Gegenstand des Verarbeitung</b>	<b>16</b>
<b>§ 3: Dauer des Auftrags</b>	<b>16</b>
§ 3.1: Sonderkündigungsrecht	17
<b>§ 4: Verantwortlichkeiten</b>	<b>17</b>
§ 4.1: Gewährleistung Betroffenenrechte	18
§ 4.2: Bereitstellung gemäß Art. 26 Abs. 2 DS-GVO	18
§ 4.3: Funktionen der Verarbeitung	19
<b>§ 5: Pflichten bei der Verarbeitung</b>	<b>19</b>
§ 5.1: Allgemeine Pflichten	19
§ 5.2: Gewährleistung der Vertraulichkeit	20
§ 5.3: Gewährleistung der Sicherheit der Verarbeitung	20
§ 5.4: Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern	20

<b>§ 6:</b>	<b>Auftragsverarbeitung</b>	<b>21</b>
<b>§ 7:</b>	<b>Haftung</b>	<b>21</b>
<b>§ 8:</b>	<b>Salvatorische Klausel</b>	<b>22</b>
<b>§ 9:</b>	<b>Rechtswahl, Gerichtsstand</b>	<b>22</b>
<b>Anhang 1:</b>	<b>Zu ergreifende technische und organisatorische Maßnahmen</b>	<b>23</b>
Anhang 1.1:	Allgemeine Maßnahmen	23
Anhang 1.2:	Pseudonymisierung	23
Anhang 1.3:	Verschlüsselung	23
Anhang 1.4:	Gewährleistung Vertraulichkeit	23
Anhang 1.5:	Gewährleistung Integrität	24
Anhang 1.6:	Gewährleistung Verfügbarkeit	24
Anhang 1.7:	Gewährleistung Belastbarkeit	25
Anhang 1.8:	Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung	25
<b>Anhang 2:</b>	<b>Ansprechpartner für Datenschutz</b>	<b>26</b>

## Zusammenfassung

Manchmal erfolgt eine gleichberechtigte Zusammenarbeit verschiedener Unternehmen, Institutionen oder Behörden im Rahmen einer einzelnen Verarbeitungstätigkeit zur Erreichung eines gemeinsamen Zieles. Die Datenschutz-Grundverordnung (DS-GVO) adressiert diese Form der gemeinsamen Zusammenarbeit durch den in Art. 26 DS-GVO zu findenden Begriff der „gemeinsam für die Verarbeitung Verantwortliche“ (engl. Joint controllers). In Art. 26 Abs. 1 DS-GVO heißt es: „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche.“

Die gemeinsame Verarbeitung ist von der Auftragsverarbeitung oder Funktionsübertragung zu trennen bzw. abzugrenzen. Bei der gemeinsamen Verarbeitung entscheiden zwei oder mehr Stellen gleichberechtigt über die Zwecke und Mittel der Verarbeitung, bei der Auftragsverarbeitung entscheidet nur der Auftraggeber über Zwecke und Mittel, bei der Funktionsübertragung entscheidet jeder Verantwortliche über seine Verarbeitung völlig unabhängig von den anderen Verantwortlichen bzgl. seiner Verarbeitung.

Art. 26 DS-GVO regelt die Zulässigkeit und die Modalitäten der Durchführung einer Verarbeitung durch gemeinsam Verantwortliche, stellt jedoch keine Erlaubnisnorm für die Verarbeitung dar. Insbesondere muss der Verantwortliche bzw. müssen die Verantwortlichen i.S.v. Art. 4 Ziff. 7 DS-GVO auch die in Art. 5 DS-GVO enthaltenen „Grundsätze für die Verarbeitung personenbezogener Daten“ gewährleisten.

Art. 26 DS-GVO beinhaltet für diese Fälle der „gemeinsamen Verarbeitung“ konkrete Vorgaben, die bezogen auf den jeweiligen Sachverhalt umgesetzt werden müssen. Art. 26 Abs. 1 S. 2 DS-GVO verlangt, dass die gemeinsam Verantwortlichen eine Vereinbarung hinsichtlich ihrer gemeinsamen Verarbeitung treffen. ErwGr. 79 DS-GVO verlangt dabei eine klare Zuteilung der jeweiligen Verantwortlichkeiten, was u.a. eine Darstellung der jeweiligen tatsächlichen Funktionen und Beziehungen der jeweiligen Verantwortlichen gegenüber den Betroffenen erfordert. Weiterhin fordert Art. 26 Abs. 2 S. 2 DS-GVO, dass betroffenen Personen das „Wesentliche“ der Vereinbarung hinsichtlich gemeinsamen Verarbeitung zur Verfügung gestellt werden muss.

In dieser Ausarbeitung wird dargestellt, wann und wie diese datenschutzrechtliche Möglichkeit des „Gemeinsam Verantwortlichen“ genutzt werden kann. Insbesondere findet sich am Ende der Ausarbeitung ein Beispiel, wie eine von Art. 26 DS-GVO geforderten Vereinbarung aussehen könnte; wie jedes Beispiel ist auch dieses natürlich nicht 1:1 auf reale Gegebenheiten übertragbar, sondern muss auf die jeweiligen konkreten Anforderungen des vorliegenden Einzelfalles angepasst werden.

# 1 Einleitung

Nicht in jedem Szenario, in welchem Unternehmen oder Institutionen zusammen Daten verarbeiten, erfolgt eine Auftragsverarbeitung. Mitunter erfolgt eine gleichberechtigte Zusammenarbeit, in welcher Partner „A“ und „B“ unterschiedliche Teile der Verarbeitung übernehmen, um ein gemeinsames Ziel zu erreichen. Sowohl in der medizinischen Versorgung wie auch in der Forschung können solche Konstellationen auftreten.

Die Datenschutz-Grundverordnung (DS-GVO) adressiert diese Form der Zusammenarbeit durch den in Art. 26 DS-GVO zu findenden Begriff der „gemeinsam für die Verarbeitung Verantwortliche“ (engl. Joint controllers). Bei dieser Rechtsfigur sind zwei oder mehr natürliche oder juristische Personen gemeinsam für die Verarbeitung verantwortlich, d.h. sie entscheiden gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten (Art. 4 DS-GVO).

Den Begriff der gemeinsamen Datenverarbeitung gab es auch schon in Art. 2 lit. d EU Datenschutz-Richtlinie 95/46/EG<sup>1</sup>. Allerdings fand diese Regelung – wie manches andere auch – nie den Einzug in das deutsche Rechtssystem, d.h. diese Richtlinien-Vorgabe wurde in Deutschland nie umgesetzt. Somit wurde die Rechtsfigur des „gemeinsamen Verantwortliche“ auch nicht ins BDSG a.F. aufgenommen.

Durch die unmittelbare Anwendbarkeit der DS-GVO kommt es daher erst jetzt dazu, dass das Konstrukt der gemeinsamen Datenverarbeitung in Deutschland genutzt werden kann.

Um sich dieser, für Deutschland neuen Regelung zu nähern, ist die Stellungnahme der Artikel-29-Datenschutzgruppe zum Umgang mit dieser Thematik der Richtlinie auf Grund der nahezu wortgleichen Regelung in Art. 4 Ziff. 7 DS-GVO als Interpretationshilfe genutzt werden<sup>2</sup>, auch wenn die Regelungen in Art. 26 DS-GVO zu dieser Thematik weit umfassender sind, als die Regelungen der Richtlinie.

Im Nachfolgenden soll dargestellt werden, wann und wie dieses Konstrukt sinnvoll eingesetzt werden kann. Insbesondere findet sich am Ende der Ausarbeitung ein Muster für eine von Art. 26 DS-GVO geforderten Vereinbarung, um dem Leser eine Vorstellung bzgl. der Anforderungen einer derartigen Vereinbarung zu geben. Das Muster kann hierbei nur als ein Beispiel dienen. Wir wollen daher darauf hinweisen, dass eine solche Vereinbarung immer auf die jeweiligen Anforderungen der vorliegenden, konkreten Begebenheiten des Einzelfalles angepasst werden muss.

Hinweis zur Benutzung: Alternative Textpassagen werden durch die Abkürzung „Alt.“, optionale Textteile durch die Abkürzung „Opt.“ hervorgehoben.

---

<sup>1</sup> Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Online, zitiert am 2018-06-12; Verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31995L0046>

<sup>2</sup> Artikel-29-Datenschutzgruppe. (2010) WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. Online, zitiert am 2018-06-12; Verfügbar unter [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm) bzw. direkt dt. pdf-Datei unter [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf)

## 2 Erläuterungen zum rechtlichen Hintergrund

Entsprechend ErwGr. 79 bedarf es auch in Konstellationen, in denen ein Verantwortlicher die Zwecke und Mittel der Verarbeitung gemeinsam mit anderen Verantwortlichen festlegt, einer klaren Zuteilung der Verantwortlichkeiten. Art. 26 DS-GVO beinhaltet für diese Fälle der „gemeinsamen Verarbeitung“ konkrete Vorgaben, die bezogen auf den jeweiligen Sachverhalt umgesetzt werden müssen.

### 2.1 Definition „gemeinsam Verantwortliche“

Art. 4 Ziff. 7 DS-GVO definiert einen (gemeinsamen) Verantwortlichen als jemanden, der allein oder *gemeinsam mit anderen über die Zwecke und Mittel* der Verarbeitung von personenbezogenen Daten entscheidet. Dies findet sich so auch in Art. 26 Abs. 1 S.1 DS-GVO wieder, in dem es heißt: „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche.“

Dabei kommt es bei der Beurteilung der Tatsache, ob die Parteien gemeinsam über Zwecke und Mittel bestimmen können, weniger auf die vertragliche Ausgestaltung an, sondern vielmehr ist entscheidend für diese Beurteilung, dass eine solche Entscheidungsbefugnis in der Realität auch tatsächlich gegeben ist. Damit kommt es hinsichtlich der Beurteilung maßgeblich auf die Betrachtung und Bewertung anhand der tatsächlichen Gegebenheiten an<sup>3</sup>.

Gemäß der Interpretation der Artikel -29-Datenschutzgruppe muss der Begriff „gemeinsam“ „im Sinne von ‚zusammen mit‘ oder ‚nicht alleine‘ in unterschiedlichen Spielarten und Konstellationen ausgelegt werden“<sup>4</sup>. Wie der EuGH in seinem Facebook-Urteil feststellte, muss nicht jeder der Verantwortlichen gleich viel Verantwortung haben und über alle Daten verfügen, damit von einer gemeinsamen Verantwortung gesprochen werden kann<sup>5</sup>.

Um den Vorgaben von Art. 26 DS-GVO zu genügen, ist es daher unabdingbar, dass die jeweiligen an der gemeinsamen Verarbeitung beteiligten Parteien auch tatsächlich über die Zwecke und Mittel entscheiden bzw. entscheiden können; eine weisungsgebundene Tätigkeit wird somit nicht adressiert. Nicht zu dieser Regelung hingegen zählen Vorgänge, bei denen mehrere Verarbeitungen mit jeweils selbstständigen Verantwortlichkeiten nebeneinander vorliegen<sup>6</sup>.

#### 2.1.1 Abgrenzung zur Auftragsverarbeitung

Die gemeinsame Verarbeitung ist von der Auftragsverarbeitung zu trennen bzw. abzugrenzen. Dies kann sich in Einzelfällen, ohne entsprechende genaue Analyse des Einzelsachverhalts, als ein kompliziertes Unterfangen erweisen.

---

<sup>3</sup> Hartung J. Art. 26 Rn. 14 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

<sup>4</sup> Artikel-29-Datenschutzgruppe. (2010) WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, Abschnitt III.1.d) Zweites Element: „allein oder gemeinsam mit anderen“, S. 22. Online, zitiert am 2018-06-12; Verfügbar [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf)

<sup>5</sup> Europäischer Gerichtshof (EuGH). Urt. V. 05. Juni 2018, AZ: C-210/16. Rn. 38. Online, zitiert am 2018-06-12; Verfügbar unter <http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=d &mode=lst&dir=&occ=first&part=1&cid=568857>

<sup>6</sup> Tinnefeld C, Hanßen H. Art. 26 Rn. 8 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0

Eine Auftragsverarbeitung liegt vor, wenn der Verantwortliche konkrete Weisungen an eine andere Stelle richtet und diese Stelle Verarbeitungstätigkeiten entsprechend dieser Weisung ausführt. Daraus folgt zwangsläufig, dass immer dann, wenn eine Stelle der anderen eine Weisung hinsichtlich der Verarbeitung erteilt bzw. alleine über die Zwecke und Mittel der konkreten Datenverarbeitung entscheidet, eine gemeinsame Verarbeitung nicht vorliegen kann.

Bei der gemeinsamen Verarbeitung entscheiden zwei oder mehr Stellen gleichberechtigt über die Zwecke und Mittel der Verarbeitung. Es ist jedoch im Bereich der gemeinsamen Verantwortlichkeit möglich, dass die Verarbeitung untereinander aufgeteilt wird, so dass jede der Parteien nur eine Teilverarbeitung übernimmt und durch diese Aufteilung der Verarbeitung der (gemeinsame) Zweck der Verarbeitung erreicht wird. Dabei kann innerhalb dieser Teilverarbeitung jede Partei weisungsfrei arbeiten oder auch an gemeinsam getroffene Weisungen gebunden sein. Aber Mittel und Zwecke der Verarbeitung wurden gemeinsam festgelegt.

### 2.1.2 Beispiele

Biometrische Auswertung im Rahmen einer Studie

- a) Ein Biometriker führt im Rahmen einer Studie eine statistische Untersuchung durch. Sowohl die Fragestellung als auch die Daten, die ihm für die Auswertung zur Verfügung stehen, sind von anderen vorgegeben. Da dem Biometriker hinsichtlich der Verarbeitung klare Vorgaben aufgegeben wurden und er insbesondere nicht über die Mittel und Zwecke der Verarbeitung entscheidet, liegt eine Auftragsverarbeitung vor.
- b) Ein Biometriker arbeitet gemeinsam mit anderen Forschern an einem Projekt. Vor Beginn der Studie legen sie gemeinsam die in der Studie zu beantwortenden / zu behandelnden Fragestellungen fest, der Biometriker entscheidet, welche Daten im Rahmen der Forschung erhoben werden müssen, damit er eine qualifizierte Auswertung durchführen kann. Die Daten werden von den anderen Forschern erhoben und zur Auswertung dem Biometriker übergeben. Hier findet eine gemeinsame Verarbeitung statt, der Biometriker als auch seine Forscherkollegen sind bzgl. Entscheidung hinsichtlich Zwecke und Mittel des Forschungsvorhabens gemeinsam-verantwortlich.

Bereitstellung von Daten in einer Datenbank

- a) In einer (gemeinsamen) Datenbank, z.B. in einer zentralen elektronischen Patientenakte, stehen Daten zum Abruf bereit. Mehrere voneinander unabhängige Stellen können in dieser Datenbank Daten speichern, ändern und/oder abrufen. Jedoch legt die die Infrastruktur und damit die Daten bereitstellende Stelle fest, welche Datenkategorien gespeichert werden können. Hier liegt keine gemeinsame Verarbeitung i.S.v. Art. 26 DSGVO vor, da die die datenbereitstellende Stelle festlegt, welche Datenkategorien gespeichert werden. D.h. nur diese Stelle bestimmt über die Mittel und Zwecke der Verarbeitung.
- b) In einer (gemeinsamen) Datenbank, z.B. in einer zentralen elektronischen Patientenakte, stehen Daten zum Abruf bereit. Die Kooperationspartner legten gemeinsam fest, welche Datenkategorien verarbeitet werden, d.h. von wem sie gespeichert, geändert und/oder abgerufen werden können. All dieses wurde in einem Kooperationsvertrag festgehalten. Hier liegt eine gemeinsame Verantwortlichkeit vor, denn es wird gemeinsam über Mittel und Zwecke entschieden.



Klinische Studie<sup>7</sup> (Arzneimittel, Medizinprodukt)

- a) Prüfer (i.S.v. § 4 Ziff. 25 AMG, § 3 Ziff. 24 MPG) arbeiten i.d.R. auf Weisung, d. h. die Zwecke der Verarbeitung werden ihnen vom Sponsor vorgegeben, sie können jedoch nicht (frei) darüber bestimmen<sup>8</sup>. Insofern liegt in der Regel bei diesen eine Auftragsverarbeitung vor.
- b) Der Sponsor als die für die Veranlassung, Organisation und Finanzierung einer klinischen Prüfung verantwortliche natürliche oder juristische Person einer klinischen Studie (vgl. § 4 Ziff. 24 AMG, § 3 Ziff. 23 MPG) ist datenschutzrechtlich immer ein Verantwortlicher. Daraus folgt, dass immer, wenn mehr als ein Sponsor an einem Studienvorhaben beteiligt sind, diese datenschutzrechtlich als gemeinsame Verantwortliche anzusehen sind.

## 2.2 Erlaubnistatbestand

Art. 26 DS-GVO regelt die Zulässigkeit und die Modalitäten der Durchführung einer Verarbeitung durch gemeinsam Verantwortliche, stellt jedoch keine Erlaubnisnorm für die Verarbeitung dar. Daher muss für die Zulässigkeit der Verarbeitung immer ein Erlaubnistatbestand existieren, der die Datenverarbeitung legitimiert. Dieser muss entweder in Art. 6 Abs. 1 DS-GVO stehen oder, wenn es sich um die Verarbeitung besonderer Kategorien personenbezogener Daten handelt, in Art. 9 Abs. 2 DS-GVO.

Insbesondere muss der Verantwortliche bzw. müssen die Verantwortlichen i.S.v. Art. 4 Ziff. 7 DS-GVO auch die in Art. 5 DS-GVO enthaltenen „Grundsätze für die Verarbeitung personenbezogener Daten“ gewährleisten. Daraus folgt, dass i.d.R. jeder Verantwortliche einen Erlaubnistatbestand für seinen Teil der Verarbeitung benötigt. Kann nur ein Verantwortlicher einen Erlaubnistatbestand aus den datenschutzrechtlichen Vorgaben ableiten, so spricht vieles dafür, dass es sich bei der Verarbeitung um eine Verarbeitung im Auftrag des einen Verantwortlichen handelt.

Letztlich muss daher jede der an der Verarbeitung beteiligten Parteien eine Erlaubnis für ihren Teil der Verarbeitung haben. Dieses ist stets auch ein prägender Teil der Begrifflichkeit „Gemeinsame Verantwortliche“.

## 2.3 Vereinbarung zwischen gemeinsam Verantwortlichen

Art. 26 Abs. 1 S. 2 DS-GVO verlangt, dass die gemeinsam Verantwortlichen eine Vereinbarung hinsichtlich ihrer gemeinsamen Verarbeitung treffen. Dabei ist keine bestimmte Form vorgeschrieben, jedoch muss entsprechend Art. 5 Abs. 2 DS-GVO der Nachweis bzgl. des Vorliegens einer der Vereinbarung sowie der vereinbarten Inhalte geführt werden (können).

ErwGr. 79 DS-GVO verlangt darüber hinaus eine *klare* Zuteilung der jeweiligen Verantwortlichkeiten. Sowohl im Hinblick auf die aus diesem Erwägungsgrund resultierende Forderung nach einer transparenten Regelung wie auch den oben dargestellten bestehenden Nachweispflichten

---

<sup>7</sup> Die DFG empfiehlt auch bei nicht gesetzlich geregelten klinischen Studien die Verantwortlichkeiten klar zu benennen. Siehe: DFG (2011) Grundsätze und Verantwortlichkeiten bei der Durchführung klinischer Studien. Online, zitiert am 2018-06-14; Verfügbar unter [http://www.dfg.de/download/pdf/foerderung/programme/klinische\\_studien/klinische\\_studien\\_grundsaeetze\\_verantwortlichkeiten.pdf](http://www.dfg.de/download/pdf/foerderung/programme/klinische_studien/klinische_studien_grundsaeetze_verantwortlichkeiten.pdf)

<sup>8</sup> Hinweise zu den Aufgaben der Prüfer findet sich in der Ausarbeitung des Arbeitskreises Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland e.V.: „Empfehlungen zur Bewertung der Qualifikation von Prüfern und Geeignetheit von Prüfstellen durch Ethik-Kommissionen bei klinischen Prüfungen nach dem AMG“. Online, zitiert am 2018-06-14; Verfügbar unter [http://www.ak-med-ethik-komm.de/index.php?option=com\\_content&view=article&id=144&Itemid=151&lang=de](http://www.ak-med-ethik-komm.de/index.php?option=com_content&view=article&id=144&Itemid=151&lang=de)

hinsichtlich der getroffenen Regelungen ist deshalb zu einer verbindlichen Vereinbarung in Schrift- oder Textform zu raten<sup>9</sup>. Hierbei kann natürlich auch eine elektronische Form gewählt werden, solange diese den Anforderungen bzgl. der Nachweispflicht genügt<sup>10</sup>.

Der notwendige Mindestinhalt, den eine solche Vereinbarung haben sollte, ergibt sich aus dem Wortlaut von Art. 26 DS-GVO:

- Art. 26. Abs. 1 S. 2 DS-GVO verlangt die Festlegung, welcher Verantwortliche welche Verpflichtungen der DS-GVO erfüllt.
  - o Dies gilt insbesondere hinsichtlich der aus Artt. 11 bis 22 resultierenden Betroffenenrechte. Dabei hob der europäische Gesetzgeber insbesondere die aus Artt. 13 und 14 resultierenden Informationspflichten hervor, d.h. in der Vereinbarung muss eindeutig benannt werden, welche Partei diesen Pflichten nachzukommen hat.
- Art. 26 Abs. S. 1 DS-GVO fordert eine Darstellung der jeweiligen tatsächlichen Funktionen und Beziehungen der jeweiligen Verantwortlichen gegenüber den Betroffenen.
- Ferner bietet Art. 26. Abs. 1 S. 3 DS-GVO den gemeinsamen Verantwortlichen die Möglichkeit, eine Anlaufstelle für betroffene Personen einzurichten. Jedoch resultiert allein aus der Einrichtung dieser Anlaufstelle nicht, dass nur diese für die Rechte der Betroffenen verantwortlich ist<sup>11</sup>; ein Betroffener kann auch trotz Einrichtung einer solchen Stelle seine Rechte gegenüber jedem der Verantwortlichen einzeln geltend machen. Bei der Einrichtung einer solchen Anlaufstelle handelt es sich eher um eine „Serviceleistung“ gegenüber den betroffenen Personen, welche die zentrale Annahme und interne Verteilung zur Abarbeitung der Anfragen anbietet und durchführt<sup>12</sup>.

## 2.4 Information betroffener Personen

Art. 26 Abs. 2 S. 2 DS-GVO verlangt, dass betroffenen Personen das „Wesentliche“ der Vereinbarung hinsichtlich gemeinsamer Verarbeitung zur Verfügung gestellt werden muss.

Aus dieser Forderung wird ersichtlich, dass betroffenen Personen nicht sämtliche Einzelheiten über die gemeinsame Verarbeitung offenbart werden müssen<sup>13</sup>. Somit ist es durchaus legitim, etwaige Firmengeheimnisse (z.B. finanzielle Vereinbarung zwischen den Verantwortlichen) vor dem Betroffenen geheim zu halten.

Die zur Verfügung gestellten Informationen sollten die Verarbeitung für die betroffene Person transparent im Sinne von Art. 5 Abs. 1 lit. a DS-GVO darstellen. Hierzu sollten diese Informationen insbesondere die nachfolgenden Fragen beantworten:

- Wer verarbeitet welche Daten wozu?
- Welcher Verantwortliche übt welche Funktionen aus, welcher Verantwortliche hat welche Beziehungen zu den betroffenen Personen? (i.S. Art. 26 Abs. 1 DS-GVO))

---

<sup>9</sup> Hartung J. Art. 26 Rn. 20 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

<sup>10</sup> Tinnefeld C, Hanßen H. Art. 26 Rn. 12 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0

<sup>11</sup> Hartung J. Art. 26 Rn. 21 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

<sup>12</sup> Martini M. Art. 26 Rn. 29 in Paal/Pauly (Hrsg.). Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C.H.Beck Verlag, 2. Aufl. 2018. ISBN 978-3-406-71838-0

<sup>13</sup> <sup>13</sup> Martini M. Art. 26 Rn. 31 in Paal/Pauly (Hrsg.). Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C.H.Beck Verlag, 2. Aufl. 2018. ISBN 978-3-406-71838-0

- Wer ist Ansprechpartner?
- Wie werden die Betroffenenrechte gewährleistet?
- Wie sind die Daten betroffener Personen geschützt?
- Wie wird mit Datenschutzvorfällen („Datenpannen“) umgegangen?

Art. 26 verlangt, dass diese Informationen betroffenen Personen „zur Verfügung“ gestellt werden. Damit existiert auch diesbezüglich keine Formvorgabe. Daher dürfte es ausreichen, die Informationen betroffenen Personen in Form von Datenschutzhinweisen z.B. online auf der Webseite zur Verfügung zu stellen<sup>14</sup>. Dabei müssen die Informationen von der betroffenen Person gut zu finden sein; ein „versteckter Hinweis“ auf die Erklärung oder die Einbettung in einem unübersichtlichen Menü wird den rechtlichen Anforderungen nicht genügen.

## 2.5 Rechte der betroffenen Person

Gemäß Art. 26 Abs. 3 DS-GVO kann eine betroffene Person ihre in der DS-GVO genannten Rechte gegenüber jedem einzelnen der Verantwortlichen geltend machen, ungeachtet evtl. bestehender Vereinbarungen zwischen den gemeinsam Verantwortlichen (siehe hierzu auch die Ausführungen bzgl. der Thematik einer Anlaufstelle in Abschnitt 2.2.).

## 2.6 Beschränkung

Die in Art. 26 DS-GVO eingeräumte Gestaltungsfreiheit der an der Verarbeitung gemeinsam beteiligten Parteien kann durch abweichende nationale Regelungen der Mitgliedsstaaten eingeschränkt werden, Art. 26 Abs. 1 S. 2 DS-GVO enthält hier eine entsprechende Öffnungsklausel. . Nach derzeitigem Kenntnisstand der Verfasser wurde in Deutschland von dieser Möglichkeit bisher noch kein Gebrauch gemacht.

## 2.7 Zuständige Aufsichtsbehörde

Die DS-GVO legt nicht fest, welche Behörde federführende Aufsichtsbehörde in den Fällen ist, in denen zwei oder mehr gemeinsam Verantwortliche die Zwecke und Mittel festlegen<sup>15</sup>. Der Europäische Datenschutzausschuss empfiehlt daher gemeinsam Verantwortlichen festzulegen, „welche entscheidungsbefugte Niederlassung eines gemeinsam Verantwortlichen die Befugnis haben soll, für alle gemeinsam Verantwortlichen Entscheidungen über die Datenverarbeitung umzusetzen“. Diese Niederlassung gilt dann als zuständige Hauptniederlassung der gemeinsam Verantwortlichen und daraus resultiert dann die federführende Aufsichtsbehörde.

## 2.8 Haftung

Art. 82 DS-GVO regelt den Anspruch einer betroffenen Person auf Schadenersatz, wenn der betroffenen Person auf Grund eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist. Dabei haftet jeder Verantwortliche für diesen Schaden (Art. 82 Abs. 2 S. 1 DS-GVO), ein Auftragsverarbeiter nur unter den Bedingungen von Art. 82 Abs. 2 S. 2 DS-GVO.

<sup>14</sup> Hartung J. Art. 26 Rn. 26 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

<sup>15</sup> Europäischer Datenschutzausschuss (2018) Federführende Aufsichtsbehörd. Online, zitiert am 2018-06-14; Verfügbar unter [https://edpb.europa.eu/our-work-tools/our-documents/guideline/lead-supervisory-authority\\_de](https://edpb.europa.eu/our-work-tools/our-documents/guideline/lead-supervisory-authority_de)

Verweis auf Artikel-29-Datenschutzgruppe (2017) WP244 Rev. 01 „Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters“, Kap. 2.1.3. Online, zitiert am 2018-06-14; Verfügbar unter [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611235](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235)

Dabei haftet jeder Verantwortlicher und jeder Auftragsverarbeiter gemäß Art. 82 Abs. 4 DS-GVO für den gesamten Schaden („gesamtschuldnerischen Haftung“), wodurch ein wirksamer Schutz für den Schadensersatzanspruch der betroffenen Person gewährleistet werden soll.

Um Befreiung von einer Haftung (im Innenverhältnis) zu erzielen, muss jeder Verantwortliche bzw. jeder Auftragsverarbeiter nachweisen, dass sie nicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind. Daher sollten in der Vereinbarung zur gemeinsamen Verarbeitung auch Regelungen existieren, wie im Innenverhältnis die Haftung geregelt wird.

## 2.9 Sanktionierung

Gemäß Art. 83 Abs. 4 lit. a DS-GVO kann ein Pflichtversäumnis bzw. ein Verstoß gegen die Vorgaben des Art. 26 DS-GVO mit dem „kleinen“ Bußgeld geahndet werden, d. h. mit einem Bußgeld bis zu 10.000.000 Euro oder - im Fall eines Unternehmens - von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.

In erster Linie ist hier die Durchführung einer gemeinsamen Datenverarbeitung ohne Abschluss einer entsprechenden Vereinbarung zu nennen. Doch ist es auch denkbar, dass ein Bußgeld verhängt werden kann, wenn zwar eine Vereinbarung der Form nach vorliegt, jedoch von Art. 26 DS-GVO geforderte Aspekte nicht oder nicht ausreichend abgebildet worden sind. Und selbstverständlich muss die Vereinbarung die Aufteilung der Verantwortlichkeiten auch wahrheitsgetreu abbilden, und dabei insbesondere die Funktionen und Beziehungen der Verantwortlichen gegenüber betroffenen Personen wahrheitsgetreu wiedergeben<sup>16</sup>. Sollte dies nicht der Fall sein, stellt dies ebenfalls einen bußgeldbewährten Verstoß dar.

Im Nachfolgenden finden Sie eine Checkliste, in der die für eine gemeinsame Verarbeitung relevanten Aspekte in Fragenform zusammengestellt sind.

---

<sup>16</sup> Martini M. Art. 26 Rn. 30 in Paal/Pauly (Hrsg.). Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C.H.Beck Verlag, 2. Aufl. 2018. ISBN 978-3-406-71838-0

## 3 Checklisten: Was vorab zu prüfen ist

### 3.1 Allgemeine Fragen

- 1) Wer sind die an der Datenverarbeitung beteiligten Stellen?
- 2) Einigen sich alle beteiligten Stellen gleichermaßen auf Zweck und Mittel der Verarbeitung, indem alle gleichermaßen festlegen, wie die Datenverarbeitung erfolgt?
  - a. Wer gehört zu den gemeinsamen Verantwortlichen?
  - b. Wer ist Auftragsverarbeiter?
  - c. Wo liegt ggf. eine Funktionsübertragung vor?
- 3) Existiert eine Vereinbarung entsprechend Art. 26 Abs. 1 DS-GVO?
- 4) Wurde geregelt wer im Innenverhältnis wofür haftet?
- 5) Wurde festgelegt, welcher Sitz von welchem Verantwortlichen als Hauptniederlassung gilt und somit die zuständige Aufsichtsbehörde festgelegt?
- 6) Betrifft die Verarbeitung besondere Arten personenbezogener Daten?
- 7) Ist gewährleistet, dass die Betroffenenrechte jederzeit erfüllt werden können?
- 8) Gibt es eine (detaillierte) Verfahrensdokumentation sowie ein Verzeichnis der Verarbeitungstätigkeiten?
- 9) Existiert ein (ausdifferenziertes) Zugriffs- und Berechtigungskonzept?
- 10) Welche technisch-organisatorischen Maßnahmen nach Art. 32 DS-GVO wurden vereinbart und umgesetzt?
  - a. Erfolgt eine regelmäßige und dokumentierte Überprüfung der Maßnahmen?
- 11) Werden alle Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 5 DS-GVO dokumentiert?
- 12) Ist ein Prozess zur Benachrichtigung bei Verletzungen des Schutzes personenbezogener Daten vorgesehen?
  - a. Benachrichtigung der Aufsichtsbehörden?
  - b. Benachrichtigung betroffener Personen?
- 13) Erfolgt eine Information der betroffenen Personen über die gemeinsam Verantwortlichen?
- 14) Wird betroffenen Personen das Wesentliche der gemeinsamen Vereinbarung auf transparente Weise zur Verfügung gestellt?

### 3.2 Abgrenzung Verantwortlichkeiten / Beteiligung an der Verarbeitung

Pflicht	Verantwortlicher 1	Verantwortlicher 2
Festlegung der Zwecke und Mittel zur Verarbeitung	X	X
Festlegung der zu verarbeitenden Daten(-kategorien)	X	X
Festlegung, wer welche Pflichten aus der DS-GVO erfüllt	X	X
Wer fungiert als Anlaufstelle für die betroffenen Personen?		
Wer stellt betroffenen Personen das Wesentliche der Vereinbarung zur Verfügung?		
Wer ist für die Informationspflicht nach Art. 13 DS-GVO verantwortlich?		
Wer ist für die Informationspflicht nach Art. 14 DS-GVO verantwortlich?		
Wer beantwortet Auskunftsanfragen nach Art. 15 DS-GVO?		
Wer bearbeitet auf Art. 16 DS-GVO beruhende Berichtigungsanfragen ?		
Wer bearbeitet auf Art. 17 DS-GVO beruhende Löschungsanfragen ?		
Wer bearbeitet auf Art. 18 DS-GVO beruhende Aufforderungen zur Einschränkung der Verarbeitung?		
Wer gewährleistet die Erfüllung der Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Sperrung gemäß Art. 19 DS-GVO?		
Wer gewährleistet das Recht auf Datenübertragbarkeit gemäß Art. 20 DS-GVO?		
Wer bearbeitet auf Art. 21 DS-GVO beruhende Widersprüche zur Verarbeitung?		
Wer setzt wie die aus Art. 25 DS-GVO resultierende Anforderung „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ um?		
Wer führt, sofern erforderlich, eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO durch?		
Wer gewährleistet die Sicherheit der Verarbeitung entsprechend Art. 32 DS-GVO		
Wer führt das Verzeichnis der Verarbeitungstätigkeiten?		
Wer gewährleistet die aus Art. 33 DS-GVO resultierende Meldepflicht bei Datenpannen?		
Wer gewährleistet die aus Art. 34 DS-GVO resultierende Meldepflicht bei Datenpannen?		
Ist ein Datenschutzbeauftragter benannt?		

## 4 Abkürzungen

Abs.	Absatz
a.F.	Alte Fassung
Art.	Artikel
Artt.	Artikel (Mehrzahl)
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
ErwGr.	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
i.S.v.	Im Sinne von
IT	Informationstechnik, informationstechnisches...
Kap.	Kapitel
LDSG	Landesdatenschutzgesetz
Lit.	littera (lat. „Buchstabe“)
LKHG	Landeskrankenhausgesetz
S.	Satz
TK	Telekommunikation(s-)
Ziff.	Ziffer

## 5 Literatur

### 5.1 Online

- 1) Artikel-29-Datenschutzgruppe. (2010) WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. Online, zitiert am 2018-06-12; Verfügbar unter [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm) bzw. direkt dt. pdf-Datei unter [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf)
- 2) Bitkom e.V. (2017) Leitfaden „Joint Controllershship in der EU-Datenschutz-Grundverordnung“. Online, zitiert am 2018-06-12; Verfügbar unter <https://www.bitkom.org/Bitkom/Publikationen/Joint-Controllershship-in-der-EU-Datenschutz-Grundverordnung.html>
- 3) Datenschutzkonferenz (DSK) (2018) Kurzpapier Nr. 16 - Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO. Online, zitiert am 2018-06-12; Verfügbar unter [https://www.lida.bayern.de/media/dsk\\_kpnr\\_16\\_gemeinsam\\_verantwortliche.pdf](https://www.lida.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf)
- 4)

### 5.2 Zeitschriften

- 1) Dovas MU. (2016) Joint Controllershship – Möglichkeiten oder Risiken der Datennutzung? ZD: 512-517



---

Die nachfolgend aufgeführte Vereinbarung bzgl. einer gemeinsamen Verarbeitung dient nur der Veranschaulichung, wie die Anforderungen aus Art. 26 DS-GVO umgesetzt werden können. Diese Muster-Vereinbarung erhebt keinen Anspruch auf Vollständigkeit. Insbesondere kann die Richtigkeit nicht garantiert und keine Gewährleistung übernommen werden.

---

# Muster-Vereinbarung

---

über eine gemeinsame Verarbeitung von Personenbezogenen Daten nach Art. 26 zwischen

Name  
Anschrift, vertreten durch  
(Im Folgenden „Verantwortlicher 1“ genannt)

und

Name  
Anschrift, vertreten durch  
(Im Folgenden „Verantwortlicher 2“ genannt)

## Präambel

Diese Vereinbarung regelt die Rechte und Pflichten der beiden Verantwortlichen (in Folge auch „Parteien“ genannt) in Bezug auf die gemeinsame Verarbeitung personenbezogener Daten. Dabei findet diese Vereinbarung auf alle Tätigkeiten Anwendung, bei denen Beschäftigte der Parteien oder durch sie beauftragte Auftragsverarbeiter personenbezogene Daten der Verantwortlichen verarbeiten. Die Parteien haben die Mittel und Zwecke der nachfolgend näher beschriebenen Verarbeitungstätigkeiten gemeinsam festgelegt. Insofern sind Sie gemeinsam Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO.

## § 1: Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 BDSG, § 2 UWG und § 2 TMG sowie Landesdatenschutzgesetz/Landeskrankenhausgesetz[hier bitte das jeweils geltende Rechtswerk benennen]. Sollten diese Artikeln bzw. Paragraphen sich widersprechende Regelungen beinhalten, gelten die Definitionen in der Rangfolge DS-GVO, BDSG, Landesrecht, UWG und TMG. Darüber hinaus gelten folgende Begriffsbestimmungen:

(1) Anonymisierung

Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

- (2) Drittland  
Ein Land, welches sich außerhalb der EU/EWR befindet.
- (3) Hauptvertrag  
Vertrag (i.d.R. ein Dienst- oder Werkvertrag), in welchem alle Einzelheiten der Verarbeitung beschrieben sind.
- (4) Unterauftragnehmer  
Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.
- (5) Weisung  
Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

## § 2: Gegenstand des Verarbeitung

- (1) Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch die Parteien in Ergänzung des Vertrags der Parteien vom ... (nachstehend „Hauptvertrag“ genannt“).
- (2) Die zu erbringenden Leistungen jeder Partei sind im Hauptvertrag im Abschnitt ... festgehalten.
- (3) Die Zwecke der gemeinsam durchgeführten Verarbeitung sind
  - a) ...
  - b) ...
- (4) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien
  - Personenstammdaten (z. B. Mitarbeiter, Kooperationspartner, nicht med. Patientendaten)
  - Medizinische Patientendaten (Befunde, Diagnosen, ...)
  - Kontaktdaten/Kommunikationsdaten (z. B. IP-Adressen, Telefon, E-Mail)
  - Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  - Kundenhistorie
  - Vertragsabrechnungs- und Zahlungsdaten
  - Planungs- und Steuerungsdaten
  - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
  - ...

## § 3: Dauer des Auftrags

### Alt. 1 zu Abs. 1

- (1) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieser Vereinbarung nicht etwas anderes ergibt

#### Alt. 2 zu Abs. 1

- (1) Die Verarbeitung beginnt am [DATUM] und endet am [DATUM].

#### Alt. 3 zu Abs. 1

- (1) Der Vertrag wird mit Unterzeichnung wirksam und läuft auf unbestimmte Zeit. Jede Partei ist berechtigt, die Vereinbarung mit einer Frist von ... Wochen zum Monatsende/Quartalsende/Jahresende (nicht Zutreffendes streichen) zu kündigen.

#### Alt. 4 zu Abs. 1

- (1) Der Vertrag wird mit Unterzeichnung wirksam und läuft auf unbestimmte Zeit bis zur Kündigung dieser Vereinbarung oder des Hauptvertrags durch eine Partei.

#### Alt. 4 zu Abs. 1

- (1) Der Vertrag wird mit Unterzeichnung wirksam und läuft auf unbestimmte Zeit bis zur Kündigung dieser Vereinbarung oder des Hauptvertrags durch eine Partei.

#### Alt. 4 zu Abs. 1

- (1) Die Verarbeitung beginnt am [DATUM] und endet nach einmaliger Ausführung
- (2) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt davon unberührt.
- (3) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

### § 3.1: Sonderkündigungsrecht

- (1) Beide Parteien können den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß der anderen Partei gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn eine Partei die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- (2) Bei unerheblichen Verstößen durch eine Partei setzt die andere Partei eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist sie zur außerordentlichen Kündigung berechtigt.
- (3) Im Falle der außerordentlichen Kündigung hat die Partei, die das Verschulden an der Kündigung trifft, der anderen Partei alle Kosten zu erstatten, die durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages entstehen.

### § 4: Verantwortlichkeiten

#### Alt. 1 zu Abs. 1

- (1) Beide Parteien sind gleichermaßen für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DS-GVO) verantwortlich.

#### Alt. 2 zu Abs. 1

- (1) Jede Partei gewährleistet die Einhaltung der gesetzlichen Bestimmungen, insbesondere die Rechtmäßigkeit der durch sie durchgeführten Datenverarbeitungen. Beide Parteien sind jedoch gleichermaßen für die Rechtmäßigkeit der gemeinsamen Verarbeitungen verantwortlich.

- (2) Die Parteien ergreifen alle erforderlichen technischen und organisatorischen Maßnahmen, damit die Rechte der betroffenen Personen, insbesondere nach Kapitel III DS-GVO, innerhalb der gesetzlichen Fristen jederzeit gewährleistet werden können bzw. sind.

**Alt. 1 zu Abs. 3**

- (3) Der Sitz von Verantwortlicher 1 gilt als Hauptniederlassung und als Referenz zur Bestimmung der zuständigen Aufsichtsbehörde.

**Alt. 1 zu Abs. 3**

- (3) Der Sitz von Verantwortlicher 1 gilt als Hauptniederlassung und als Referenz zur Bestimmung der zuständigen Aufsichtsbehörde.

## **§ 4.1: Gewährleistung Betroffenenrechte**

**Alt. 1 zu Abs. 1**

- (1) Verantwortlicher 1 verpflichtet sich, betroffenen Personen die gemäß Art. 13 und 14 DS-GVO verpflichtenden Informationen zukommen zu lassen.

**Alt. 2 zu Abs. 1**

- (1) Verantwortlicher 2 verpflichtet sich, betroffenen Personen die gemäß Art. 13 und 14 DS-GVO verpflichtenden Informationen zukommen zu lassen.

**Alt. 1 zu Abs. 2**

- (2) Verantwortlicher 1 verpflichtet sich, betroffenen Personen die ihnen gemäß Art. 15 DS-GVO zustehenden Informationen bei Nachfrage zur Verfügung zu stellen.

**Alt. 2 zu Abs. 2**

- (2) Verantwortlicher 2 verpflichtet sich, betroffenen Personen die ihnen gemäß Art. 15 DS-GVO zustehenden Informationen bei Nachfrage zur Verfügung zu stellen.  
(3) Die im Rahmen dieser Vereinbarung zu verarbeitenden Daten werden nur entsprechend der getroffenen vertraglichen Vereinbarung berichtigt, gelöscht oder gesperrt.

**Alt. 1 zu Opt. (4)**

- (4) Als Anlaufstelle für betroffene Personen agiert Verantwortlicher 1.

**Alt. 1 zu Opt. (4)**

- (4) Als Anlaufstelle für betroffene Personen agiert Verantwortlicher 2.

## **§ 4.2: Bereitstellung gemäß Art. 26 Abs. 2 DS-GVO**

**Alt. 1 zu Abs. 1**

- (1) Verantwortlicher 1 verpflichtet sich, betroffenen Personen die gemäß Art. 26 Abs. 2 DS-GVO verpflichtenden Informationen zukommen zu lassen. Somit muss Verantwortlicher 1 den betroffenen Personen das Wesentliche dieser Vereinbarung auf transparente Weise zur Verfügung stellen. Hierzu gehören auch die Informationen über die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gehören, insbesondere Auch die Beziehungen zu den betroffenen Personen.

**Alt. 2 zu Abs. 1**

- (1) Verantwortlicher 2 verpflichtet sich, betroffenen Personen die gemäß Art. 26 Abs. 2 DS-GVO verpflichtenden Informationen zukommen zu lassen. Somit muss Verantwortlicher 2 den

betroffenen Personen das Wesentliche dieser Vereinbarung auf transparente Weise zur Verfügung stellen. Hierzu gehören auch die Informationen über die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gehören, insbesondere Auch die Beziehungen zu den betroffenen Personen.

### § 4.3: Funktionen der Verarbeitung

(1) Verantwortlicher 1 ist für folgende Verarbeitungen verantwortlich:

- a. ...
- b. ...

(2) Verantwortlicher 2 ist für folgende Verarbeitungen verantwortlich:

- a. ...
- b. ...

Opt. (3) Eine übergreifende Zusammenarbeit zur Erreichung des Zweckes erfolgt in folgenden Teilen der gesamten Verarbeitung:

- a. ...
- b. ...

## § 5: Pflichten bei der Verarbeitung

### § 5.1: Allgemeine Pflichten

- (1) Beide Parteien müssen sich unverzüglich und vollständig informieren, wenn sie bei der Prüfung der Verarbeitungstätigkeiten und/oder der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellen.
- (2) Soweit ein Betroffener sich unmittelbar an eine der Parteien zwecks Wahrnehmung seiner Betroffenenrechte, insbesondere wegen Berichtigung und Löschung, seiner Daten wenden sollte, wird dieses Ersuchen unverzüglich unabhängig von der Pflicht zur Gewährleistung des Betroffenenrechtes an die andere Partei weitergeleitet.

Alt. 1 zu Abs. 3

- (3) Verantwortlicher 1 führt für die Verarbeitung ein Verzeichnis der Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DS-GVO.

Alt. 2 zu Abs. 3

- (3) Verantwortlicher 2 führt für die Verarbeitung ein Verzeichnis der Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DS-GVO.
- (4) Beiden Parteien obliegen die aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen gleichermaßen.
- (5) Ist eine Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO erforderlich, so wird diese von beiden Parteien gemeinsam durchgeführt.
- (6) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich zu behandeln
- (7) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch jede der Parteien entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

- (8) Jede Partei benennt eine oder einen Datenschutzbeauftragten. Sollte eine gesetzliche Pflicht zur Benennung nicht bestehen, wird ein Ansprechpartner mit entsprechenden Rechten und Pflichten benannt. Ein Wechsel der oder des Datenschutzbeauftragten resp. Ansprechpartners ist der anderen Partei unverzüglich schriftlich mitzuteilen. Die zum Abschluss dieser Vereinbarung gültigen Kontaktdaten des oder Datenschutzbeauftragten resp. Ansprechpartners sind in Anhang 2 dieser Vereinbarung aufgeführt.

## **§ 5.2: Gewährleistung der Vertraulichkeit**

- (1) Die Parteien erklären rechtsverbindlich, dass alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet wurden, oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.
- (2) Falls von der Verarbeitung etwaige durch § 203 StGB geschützte Berufsgeheimnisse von der Verarbeitung betroffen sind, erklären beide Parteien rechtsverbindlich, dass alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Verschwiegenheit nach § 203 StGB verpflichtet wurden. Alle mit der Verarbeitung beauftragten Personen wurden darüber informiert, dass die Verschwiegenheitsverpflichtung auch nach Beendigung ihrer Tätigkeit und Ausscheiden bestehen bleibt.

**Opt. (3)** Weiterhin sind alle Personen bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen der Parteien zu verpflichten und müssen vor Verarbeitungsbeginn auf § 17 UWG und die bei einem Verstoß einhergehenden Konsequenzen hingewiesen werden.

**Opt. (4)** Die Wahrung des Fernmeldegeheimnisses entsprechend §88 TKG muss von allen an der Verarbeitung Beteiligten gewahrt werden. Dazu müssen alle Personen, die auftragsgemäß auf Daten der Parteien bspw. Telefon oder E-Mail zugreifen können, vor Verarbeitungsbeginn auf das Fernmeldegeheimnis verpflichtet und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehrt werden.

## **§ 5.3: Gewährleistung der Sicherheit der Verarbeitung**

- (1) Beide Parteien verpflichten sich, in ihrem jeweiligen Verantwortungsbereich die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Jede Partei wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen. Diese Maßnahmen werden von den Parteien abgesprochen und vor Beginn der Verarbeitung abgestimmt. Die diesbezüglich abgestimmten zu ergreifenden bzw. bereits getroffenen technischen und organisatorischen Maßnahmen sind im Anhang I dieser Vereinbarung festgehalten.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es jeder Partei gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

## **§ 5.4: Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern**

- (1) Während der Gültigkeit der Vereinbarung berichtigt, löscht oder sperrt eine Partei die vertragsgegenständlichen Daten nur in Abstimmung mit der jeweils anderen Partei.

**Alt. 1 zu Abs. 2**

- (2) Sofern eine Vernichtung während der laufenden Verarbeitung vorzunehmen ist, übernimmt Verantwortlicher 2 die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien.

#### Alt. 1 zu Abs. 2

- (2) Sofern eine Vernichtung während der laufenden Verarbeitung vorzunehmen ist, übernimmt Verantwortlicher 1 die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien.

## § 6: Auftragsverarbeitung

- (1) Jede Partei verpflichtet sich, beim Einsatz von Auftragsverarbeitern mit diesen einen Vertrag nach Art. 28 DS-GVO abzuschließen. Vor Abschluss des Vertrages ist die andere Partei zu informieren.
- (2) Jede Partei hat das Recht, die Beauftragung eines bestimmten Auftragsverarbeiters bei Vorliegen wichtiger Gründe zu untersagen. Insbesondere die Hinzuziehung eines Markt-Wettbewerbers einer der Parteien kann als wichtiger Grund in diesem Sinne verstanden werden und einen wichtigen Untersagungsgrund darstellen.
- (3) Ein Auftragsverarbeiter muss vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen. Erfolgt eine Leistungserbringung durch einen Unterauftragnehmer in einem Drittland, so müssen beide Parteien ihre Zustimmung hierzu erteilt haben.
- (4) Beim Einsatz von Auftragsverarbeitern muss der jeweilige Auftragsverarbeiter zur Gewährleistung der sich aus dieser Vereinbarung ergebenden Pflichten von der den Auftragsverarbeiter beauftragenden Partei vertraglich verpflichtet werden.
- (5) Jeder Auftragsverarbeiter muss gewährleisten, dass beim Einsatz von Unterauftragnehmern die sich aus dieser Vereinbarung ergebenden Pflichten auch bei Unterauftragnehmern erfüllt werden.
- (6) Jeder Auftragsverarbeiter muss einen Datenschutzbeauftragten benannt haben. Die Kontaktdaten des Datenschutzbeauftragten werden beiden Parteien zur Verfügung gestellt.

## § 7: Haftung

- (1) Beide Parteien und jeder evtl. vorhandene Auftragsverarbeiter haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird im Außenverhältnis gemeinsam gegenüber der jeweiligen betroffenen Person.
- (2) Soweit die Parteien zum Schadensersatz gegenüber dem Betroffenen gemeinsam verpflichtet sind, bleibt jeder Partei der Rückgriff auf einen Auftragsverarbeiter vorbehalten.
- (3) Im Innenverhältnis haftet jede Partei gegenüber den anderen Parteien für den Schaden, welcher durch die von ihr zu verantwortende Verarbeitung entstand.
- (4) Im Innenverhältnis zwischen den Parteien und evtl. eingesetztem Auftragsverarbeiter haftet der Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
  - a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
  - b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.
- (5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

## § 8: Salvatorische Klausel

- (1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
- (2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
- (3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.
- (4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter § 8 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

## § 9: Rechtswahl, Gerichtsstand

- (1) Es gilt deutsches Recht.

Alt. 1 zu Abs. 2

- (2) Gerichtsstand ist der Sitz des Auftraggebers.

Alt. 2 zu Abs. 2

- (2) Gerichtsstand ist der Sitz des Auftraggebers.



# Anhang 1: Zu ergreifende technische und organisatorische Maßnahmen

## Anhang 1.1: Allgemeine Maßnahmen

- Gewährleistung Zweckbindung:
  - 
  - 
  - 
  - 
  -

## Anhang 1.2: Pseudonymisierung

- 

## Anhang 1.3: Verschlüsselung

- 

## Anhang 1.4: Gewährleistung Vertraulichkeit

- Klassifikation der Daten in die Vertraulichkeitsstufen geheim/vertraulich/intern/öffentlich
- Zutrittskontrolle:
  - 
  - 
  - 
  - 
  -
- Zugangskontrolle:
  - 
  - 
  - 
  - 
  -
- Zugriffskontrolle:
  - 
  - 
  - 
  - 
  -
- Weitergabekontrolle:
  - 
  - 
  - 
  - 
  -
- Verarbeitungskontrolle:
  -

- 
- 
- 
- 

Trennungskontrolle:

- 
- 
- 
- 
- 

## Anhang 1.5: Gewährleistung Integrität

Eingabekontrolle:

- 
- 
- 
- 

Weitergabekontrolle:

- 
- 
- 
- 
- 

Auftragskontrolle:

- 
- 
- 
- 
- 

## Anhang 1.6: Gewährleistung Verfügbarkeit

Backupkonzept:

- 
- 
- 
- 
- 

Recoverykonzept:

- 
- 
- 
- 
- 

Löschkonzept inkl. zeitliche Vorgaben zur Löschung

### **Anhang 1.7: Gewährleistung Belastbarkeit**

- Organisatorische Anforderungen
  - 
  - 
  - 
  - 
  -

- Technische Maßnahmen
  - 
  - 
  - 
  - 
  -

- Server- und Client-Absicherung
  - 
  - 
  - 
  - 
  -

### **Anhang 1.8: Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

- Regelmäßige Schulungen aller an der Verarbeitung beteiligten Personen
- Einsatz eines Datenschutz-Management-Systems sowie eine regelmäßige Auditierung desselben
- Zertifizierung ...

## Anhang 2: Ansprechpartner für Datenschutz

Verantwortlicher 1:

Name: .....

Funktion: .....

Anschrift: .....

.....

Telefon: .....

E-Mail: .....

Verantwortliche 2:

Name: .....

Funktion: .....

Anschrift: .....

.....

Telefon: .....

E-Mail: .....