Mustervertrag

Datennutzung KonsortSWD

Version 1.0.0., Stand: 20.01.2022

**Datennutzungsvertrag**

zwischen

|  |
| --- |
| ❍ der Institution \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – nachfolgend: Hauptverantwortlich Datennutzende – |

*(oder)*

|  |  |
| --- | --- |
| ❍ der natürlichen Person  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ❑ und als Angehörige/r der Institution  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – nachfolgend: Hauptverantwortlich Datennutzende – | |

❑ sowie den weiteren im **Anhang Datennutzende** bezeichneten Personen

– Datennutzende –

und

|  |
| --- |
| ❍ der Institution \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – nachfolgend: Datengebende Stelle –  – gleichzeitig Forschungsdatenzentrum (FDZ) – |

*(oder)*

|  |  |
| --- | --- |
| ❍ der Institution  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – nachfolgend: Datengebende Stelle – | unter Vermittlung durch ❍    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – nachfolgend: Forschungsdatenzentrum (FDZ) – |

*(oder)*

|  |  |
| --- | --- |
| ❍ der natürlichen Person  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ❑ und als Angehörige/r der Institution  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – nachfolgend: Datengebende Stelle – | |
| unter Vermittlung durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – nachfolgend: Forschungsdatenzentrum (FDZ) – | |

wird in Hinblick auf die in **Anhang Datenbasis** genannten Datenbestände

– Vertragsgegenstand, Datenbasis –

folgender Datennutzungsvertrag

mit der Vertragsnummer/-bezeichnung: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

geschlossen:

* 1. Hauptpflichten

#### Einräumung von Nutzungsrechten

Die Datengebende Stelle räumt den Datennutzenden das Recht ein, die Datenbasis ein eigener datenschutzrechtlicher Verantwortlichkeit und unter Einhaltung aller einschlägigen Rechtsvorschriften zu nutzen. Die Nutzungsrechte sind nicht übertragbar und nicht ausschließlich. Die Datenbasis oder Teile davon dürfen grundsätzlich nicht veröffentlicht werden. Der Umfang der Nutzungsrechte ergibt sich im Übrigen aus den nachfolgenden Bestimmungen.

#### Zugänglichmachung der Datenbasis

Das FDZ verpflichtet sich den Datennutzenden die Datenbasis gemäß dem im **Anhang Datenzugang** genannten beschriebenen Vorgehensweise zugänglich zu machen.

#### Verantwortliche Datenverarbeitung durch die Datennutzenden

Die Datennutzenden verpflichten sich, die Datenbasis in eigenem Namen und in eigener wissenschaftlicher und datenschutzrechtlicher Verantwortlichkeit zu verarbeiten. Sie geben dabei den schutzwürdigen Interessen von Personen, die von der Verarbeitung betroffen sind, im Zweifel Vorrang gegenüber eigenen Interessen. Sie kennen die neben diesem Vertrag anwendbaren rechtlichen Bestimmungen und halten sie ein und sich darüber im Klaren, dass eine Nichteinhaltung ggf. auch strafrechtliche Konsequenzen haben kann.

#### Entgelt gemäß Kostenmodell

❑ Die Datennutzenden sind zur Zahlung eines Entgeltes für die Datenbereitstellung und -zugang gemäß dem Anhang Kostenmodell verpflichtet.

* 1. Verarbeitungszweck

###### Die Datennehmenden verpflichten sich die Datenbasis …

❍ … ausschließlich zu wissenschaftlichen Zwecken

❍ … ausschließlich zu Zwecken der Lehre

❍ … ausschließlich zu dem im Anhang Vorhaben beschriebenen Zwecke

… zu nutzen und unterliegen diesbezüglich einer datenschutzrechtlichen Zweckbeschränkung

###### ❑ Eine kommerzielle Nutzung, die über die Honorare für akademische Lehr- und wissenschaftliche Tätigkeiten hinausgehen würde, ist unzulässig. Falls anderweitige wirtschaftliche Erträge unter Nutzung der Daten erzielt werden sollen, ist vorher die Zustimmung der Datengebenden Stelle einzuholen. Ohne ausdrückliches schriftliches Einverständnis des Datengebers dürfen keine Patente oder andere gewerblichen Schutzrechte, die sich auf die Daten beziehen oder durch diese begründet werden, angemeldet werden.

* 1. Nutzungsdauer

#### Reguläre Dauer der Nutzungsberechtigung

Die vorgenannten Nutzungsrechte …

❍ … werden unbefristet eingeräumt.

❍ … enden am \_\_\_\_\_\_\_\_\_, ohne dass es einer Kündigung bedarf. Eine Verlängerung dieser Frist ist auf begründeten Antrag, mindestens 4 Wochen vor Ablauf des Nutzungsrechts in beiderseitigem Einvernehmen durch schriftliche Erweiterung dieses Vertrages möglich. Die Vertragsverlängerung soll zu den Vertragsunterlagen genommen werden.

❍ … enden mit dem Abschluss des im Anhang Vorhaben beschriebenen Vorhabens, bei Abbruch des Vorhabens zum Zeitpunkt desselben.

#### Vorzeitiges Kündigungsrecht der Datengebenden Stelle

###### ❑ Der Nutzungsberechtigung kann von der Datengebenden Stelle vorzeitig ohne Angabe von Gründen mit einer Frist von 4 Wochen gekündigt werden.

###### ❑ Der Nutzungsberechtigung kann von der Datengebenden Stelle unter Bestimmung einer angemessenen Frist vorzeitig gekündigt werden, wenn sie ihrerseits zur Veranlassung der Löschung der Datenbasis verpflichtet ist. Sie soll sich in diesem Fall aktiv darum bemühen, den durch die Löschung entstehenden Schaden für die anderen Vertragsparteien so gering wie möglich zu halten.

#### Ende der Nutzungsberechtigung bei Ausscheiden und Wechsel der Institution

###### Die Datennutzenden verpflichtet sich, das FDZ unverzüglich, spätestens innerhalb von 14 Tagen, in Kenntnis zu setzen, soweit sich ihre im **Anhang Datennutzende** gemachten Angaben ändern.

###### Die Änderung ist durch Ergänzung des Anhangs zu dokumentieren. Sie ist nicht zustimmungspflichtig.

###### ❑ Das Nutzungsrecht endet, sofern Datennutzende aus der im Anhang aufgeführten jeweiligen Institution oder aus dem im Anhang beschriebenen Vorhaben ausscheiden. In diesem Fall sollen die Parteien versuchen einen neuen Vertrag abzuschließen, sofern seitens der Datennutzenden ein berechtigtes Interesse an der Weiternutzung besteht. Gleiches gilt für den Fall der Auflösung, Neugründung oder Übernahme der Institution. Der Hauptverantwortlich Datennutzende hat diese Fälle dem FDZ anzuzeigen.

#### Kündigung durch die Datennutzenden

###### Die auf sie bezogene Nutzungsberechtigung kann von den Datennutzenden ordentlich mit zwei Wochen Kündigungsfrist zum Monatsende gekündigt werden. Die Kündigung soll zum Anhang Datennutzende hinzugefügt werden.

###### ❑ Die Hauptverantwortlich Datennutzenden können die Kündigung der Nutzungsberechtigung für einzelne Datennutzende individuell und für alle Berechtigten aussprechen.

###### Etwaige Datenzugänge soll das FDZ spätestens mit einer Frist von 2 Wochen zum Monatsende, in dringenden Fällen sofort, entziehen.

* 1. Verhältnis der Vertragsparteien untereinander

#### Geltendmachung von Rechten gegenüber dem Datennutzenden

Sofern in dieser Vereinbarung nicht näher spezifiziert, können die Rechte aus dieser Vereinbarung gegenüber den Datennutzenden sowohl von der Datengebenden Stelle, als auch dem FDZ geltend gemacht werden.

#### Gemeinsame Verantwortlichkeit mehrerer Datennutzender

###### Sofern die Datennutzenden mehreren datenschutzrechtlich Verantwortlichen zuzuordnen sind, regelt diese Vereinbarung auch die gemeinsame Verantwortlichkeit dieser Verantwortlichen im Sinne von Art. 26 DSGVO. In diesem Fall sollen die Hauptverantwortlich Datennutzenden die Anlaufstelle für die Betroffenen sein. Sie soll auch verantwortlich für die Wahrnehmung der Rechte, der betroffenen Personen, inklusive der Einhaltung der Informationspflichten nach Art. 13, 14 DSGVO, sein. Die anderen Datennutzenden haben die Hauptverantwortlich Datennutzenden hierbei vollumfänglich zu unterstützen.

###### Sofern eine Verarbeitung in gemeinsamer Verantwortlichkeit mehrerer verantwortlicher Stellen erfolgt, ist das FDZ berechtigt die Namen der Verantwortlichen und die Regelungen zur Verteilung der Verantwortlichkeit zu veröffentlichen. Der Hauptverantwortlich Datennutzende kann hierzu dem FDZ weitere Informationen zur Verfügung stellen.

#### Vertretungsbefugnisse des Hauptverantwortlich Datengebenden

Die Datennutzenden erteilen dem Hauptverantwortlich Datennutzenden die Vollmacht folgende Vertragsergänzungen in Namen der Datengebenden Stelle durchzuführen:

❑ Die Aufnahme neuer Datennutzender in den Vertrag.

❑ Die Erweiterung der Datenbasis.

❑ Die Einbeziehung der EU-Standardvertragsklauseln.

❑ Die Zustimmung zur Übermittlung an Dritte zum Zwecke der Überprüfung guter wissenschaftlicher Praxis

❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Vertretungsbefugnisse des FDZ

Sofern Datengebende Stelle und FDZ auseinanderfallen, erteilt die Datengebende Stelle dem FDZ Vollmacht folgende Vertragsergänzungen im Namen der Datengebenden Stelle durchzuführen:

❑ Die Aufnahme oder Ablehnung neuer Datennutzender in den Vertrag.

❑ die Zustimmung der Erweiterung der Datenbasis.

❑ die Einbeziehung der EU-Standardvertragsklauseln.

❑ die Zustimmung zur Übermittlung an Dritte zum Zwecke der Überprüfung guter wissenschaftlicher Praxis

❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Veröffentlichungen von Ergebnissen

#### Begriffsbestimmung

###### Als Veröffentlichungen im Sinne dieses Vertrages gelten alle Dokumente die einer unbestimmten Nutzergruppe zugänglich gemacht werden. Hierzu zählen auch „graue Literatur”, „Working Papers”, „Preprints”, Veröffentlichungen in Repositorien und studentische Arbeiten, auch wenn diese nur universitätsintern veröffentlicht werden (Bachelor, Master- oder Diplomarbeiten). Darüber hinaus sind hiervon auch Präsentationsmaterialien erfasst, insbesondere wenn diese im Internet verfügbar gemacht werden.

###### ❑ Eine Ausnahme gilt nur für solche Präsentationsmaterialien, die lediglich in einem physischen Raum in kleinem, bekanntem Teilnehmerkreis dargestellt werden und ansonsten nicht weiter gegeben werden. Diese Ausnahme entbindet nicht von der datenschutzrechtlichen Geheimhaltungspflicht, sondern lediglich von Zitations-, Beleg- und etwaigen Freigabepflichten.

#### Zitation

Datennutzende müssen in allen Veröffentlichungen, die auf der Datenbasis beruhen,…

❍ …diese entsprechend der Regeln guter wissenschaftlicher Praxis zitieren. Dabei sind neben der Bezeichnung der Datenbasis und – sofern vorhanden ihrer DOI – mindestens sowohl die Datengebende Stelle/Primärforschende, also auch das FDZ zu nennen.

❍ …diese nach den Vorgaben gemäß **Anhang Zitationsregeln** zitieren.

#### Belegexemplare

❑ Dem FDZ sind kostenlos und unverzüglich – auch mit Begründung einer Verzögerung spätestens innerhalb von zwei Monaten – nach Veröffentlichung ein elektronisches Belegexemplar (PDF-Format) oder zwei papiergebundene Belegexemplare zukommen zu lassen.

* 1. Datenschutzrechtliche Pflichten und Garantien

#### Zweckbeschränkung

Die Datennutzenden verwenden die Datenbasis ausschließlich zu den in diesem Vertrag und seinen Anhängen spezifizierten Zwecken, vgl. § 2.

#### Transparenz

###### Alle Vertragsparteien verpflichten sich zur Einhaltung der für sie geltenden gesetzlichen Transparenzvorgaben bezüglich der Datenverarbeitungen, die Gegenstand dieses Vertrags sind. Auf Art 12 ff. DSGVO wird hingewiesen.

###### Das FDZ hat ein berechtigtes Interesse alle Veröffentlichungen, die auf Datenbeständen des FDZ beruhen, in eine öffentlich zugängliche Literaturliste aufzunehmen. Diese Liste dient der Information anderer Forschender sowie etwaiger Betroffener.

###### Gegen die Aufnahme in die Veröffentlichungsliste können Datennutzende in begründeten Fällen widersprechen. Der begründete Widerspruch ist spätestens mit Abgabe der Belegexemplare einzulegen.

###### Die Notwendigkeit der Speicherung der personenbezogenen Nutzerdaten beim FDZ zu Zwecken der Kommunikation, Betreuung sowie zur Kontrolle der Nutzungsverträge und für die Einhaltung von Rechenschaftspflichten ist bekannt.

###### ❑ Darüber hinaus können die von ihnen im Rahmen des Antragsverfahrens sowie des Vertragsverhältnisses gemachten Angaben, einschließlich der personenbezogenen Daten, seitens des FDZ über das Vertragsende hinaus für statistische Zwecke, an denen insoweit ein berechtigtes Interesse besteht, gespeichert werden. Hiergegen besteht ein Widerspruchsrecht.

###### ❑ Das FDZ hat ein berechtigtes Interesse die Datennutzenden auch nach Vertragsende zum Informationsaustausch und zu Befragungen im Zusammenhang mit den Aufgaben des FDZ kontaktieren. Hiergegen besteht ein Widerspruchsrecht.

###### ❑ Das FDZ ist berechtigt, die Hauptverantwortlich Datennutzenden und die Datenbasis auf die Zugriff gewährt wurde, im Internet zu veröffentlichen.

###### Bezüglich der Speicherung der Daten der Datennutzenden besteht ein Auskunftsanspruch, sowie ggf. ein Korrektur-, und Löschanspruch, sowie ein Recht auf Datenübertragbarkeit.

#### Richtigkeit und Datenminimierung

###### Die Datengebende Stelle und das FDZ verpflichten sich, die Aufbereitung, Anonymisierung und Überlassung der Datenbasis mit der üblichen und angemessenen Sorgfalt durchzuführen, übernimmt jedoch keine Gewährleistung für deren Fehlerfreiheit.

###### Die Datennutzenden sind verpflichtet, potentielle Fehler oder Mängel in der Datenbasis der Datengebenden Stelle und dem FDZ mitzuteilen. Das FDZ ist berechtigt Hinweise auf Mängel in die eigene Datendokumentation aufzunehmen. Dabei sind die berechtigten Interessen der Datennutzenden zu beachten.

###### Bei gravierenden Mängeln, soll der Datengebenden Stelle eine angemessen Frist zur Beseitigung der Mängel eingeräumt werden. Wenn eine Mängelbeseitigung nicht mehr zu erwarten ist, darf der Datennutzende vom Vertrag zurücktreten. Dieser Rücktritt hat die Wirkung, dass bereits gezahlte Entgelte zurück zu gewähren sind und das Nutzungsrecht endet.

#### Dauer / Speicherbegrenzung

###### Die Datennutzenden sind zur unverzüglichen Löschung der Datenbasis zum Ende der vereinbarten Nutzungsdauer verpflichtet. Diese Pflicht erstreckt sich auch auf sämtliche Teile der Datenbasis sowie auf Sicherungskopien, modifizierte Kopien, Auszugsdateien, Hilfsdateien und Ausdrucke der Datenbasis (im Folgenden Derivate).

###### ❑ Ausgenommen von der Löschpflicht sind solche Daten und Derivate, die kein Risiko für betroffene Personen mit sich bringen oder die keine Personenbeziehbarkeit mehr aufweisen – dies gilt regelmäßig erst dann, wenn auch einer Veröffentlichung dieser Daten keine Bedenken entgegenstünden.

###### ❑ Das FDZ verpflichtet sich zur Archivierung der Datenbasis für mindestens 10 Jahre ab Ende der vertraglichen Nutzungsdauer, um eine Überprüfung der Einhaltung guter wissenschaftlicher Praxis trotz Löschung durch die Datennutzenden zu ermöglichen. Dies gilt nur, sofern das FDZ weiterhin die notwendigen Rechte hierfür hat. Sofern aus rechtlichen Gründen eine vorzeitige Löschung erfolgt muss, muss dies den Datennutzenden mitgeteilt werden.

###### ❑ Sofern die Datengebende Stelle zur Veranlassung der Löschung der Datenbasis durch die Datennutzenden rechtlich verpflichtet ist, müssen die Datennutzenden die Löschung durchführen. Das Gleiche gilt, sofern sie gegenüber dem Betroffenen direkt verpflichtet sind.

#### Sicherheit der Datenverarbeitung

Die Datennutzenden verpflichten sich stets ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau einzuhalten. Dies geschieht in der Regel durch Einhaltung der im Anhang Technische- und organisatorische Maßnahmen beschriebenen Maßnahmen. Diese soll durch die Parteien einvernehmlich an den jeweiligen technischen Fortschritt angepasst werden. Sofern ein konkreter Bedarfsfall besteht, haben alle Parteien auch über die im vorgenannten Anhang erwähnten Maßnahmen hinaus eigenständig weitere Maßnahmen zu ergreifen.

#### Besondere Kategorien von Daten

Sofern die Datenbasis besonderer Kategorien von Daten im Sinne von Art. 9 DSGVO enthält, wird den besonderen Schutzanforderungen für die Verarbeitung durch die im Anhang Technische- und organisatorische Maßnahmen beschriebenen Schutzmaßnahmen Rechnung getragen, die insoweit der Sensibilität der Daten angepasst sind und ihr in besonderer Weise Rechnung tragen.

#### Beschränkung der Zugriffsberechtigten, Weiterübermittlung

###### Ein Zugriff auf die Datenbasis ist grundsätzlich nur für die Datennutzenden gestattet. Den Datennutzenden ist es nicht gestattet, sich bei der Haltung, Verarbeitung oder Nutzung der Datenbasis der Hilfe Dritter (Auftragnehmer, Selbständige, freiberuflich Tätige) zu bedienen; der Abschluss von einvernehmlichen Auftragsverarbeitungsverträgen wird dadurch nicht berührt.

###### Die Datennutzenden sichern zu, die Datenbasis und alle Kopien der Datenbasis geheim zu halten. Dieses Datengeheimnis besteht auch nach dem Ende der vereinbarten Nutzungsdauer fort.

###### ❑ Mitarbeitende der Hauptverantwortlich Datennutzenden können Zugriff zu der Datenbasis und der Derivate erhalten, sofern sie durch schriftliche Vereinbarung auf die Einhaltung der Pflichten dieser Vereinbarung schriftlich verpflichtet sind.

###### Eine Übermittlung zum Zweck der Überprüfung der Einhaltung guter wissenschaftlicher Praxis durch Dritte, erfolgt nur im Einvernehmen mit der Datengebenden Stelle. Diese Dritte Stelle hat die Einhaltung datenschutzrechtlicher Vorschriften zu garantieren – etwa durch eine für diesen Zweck abgeschlossene eigenständige Datennutzungsvereinbarung.

#### Auftragsverarbeitungen

Die Datennutzenden dürfen im Einvernehmen mit dem Datengeber Auftragsverarbeitungsverträge abschließen. Diese sind im **Anhang Auftragsverarbeitungen** zu dokumentieren.

#### Unterstützungspflichten

###### Die Datennutzenden erklärt sich damit einverstanden, dass die Datengebende Stelle und das FDZ berechtigt sind, die Einhaltung der vertraglichen und gesetzlichen datenschutzrechtlichen Vorschriften zu kontrollieren, insbesondere durch die Einsichtnahme zur mündlichen oder schriftlichen Verbreitung vorgesehenen Materialien und Publikationen.

###### Die Datennutzenden räumt dem FDZ das Recht ein, Auskünfte bei ihm einzuholen …

❑ … und während der Betriebs- und Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen und Prüfungen vorzunehmen, …

❑ … und auf den Vertragsgegenstand bezogene geschäftliche Unterlagen und Datenverarbeitungsprogramme einzusehen, …

… soweit dies für die Sicherstellung datenschutzrechtlicher Pflichten im Anwendungsbereich dieser Vereinbarung erforderlich ist.

###### Den Datennutzenden ist bekannt, dass Kontrollrechte auch für Aufsichtsbehörden bestehen.

#### Drittbegünstigung und Rechte betroffener Personen

❑ Allen von der Verarbeitung durch die Datennutzenden betroffenen Personen werden gegenüber den Datennutzenden mindestens die gleichen Rechte, wie sie aus gesetzlichen Bestimmungen gegenüber den Datengebenden Stellen bestehen, eingeräumt.

#### Internationale Datenübermittlungen

###### Die Verarbeitung der Datenbasis ist in allen Mitgliedstaaten der Europäischen Union sowie allen Staaten für die die Europäische Kommission nach Art. 45 Abs. 1 DSGVO die Angemessenheit des Datenschutzniveaus festgestellt hat, gestattet.

###### ❍ Sollten Datennutzende in ein Land einreisen, das ein angemessenes Datenschutzniveau nicht erfüllt, dürfen die Datennutzenden die Datenbasis und Derivate nicht mitnehmen oder auf sie zugreifen.

❍ Die Übermittlung in Drittstaaten und Verarbeitung der Datenbasis ist auf Grundlage und unter Einhaltung der EU-Standardvertragsklauseln, die diesem Vertrag als Anhang EU-Standardvertragsklauseln beigefügt ist, möglich. Die Regelungen dieser Vereinbarung gelten als Konkretisierungen der vorgenannten EU-Standardvertragsklauseln. Im Konfliktfall ist den Regeln der EU-Standardvertragsklauseln Vorrang einzuräumen.

* 1. Vertragsverstöße und Haftung

#### Begriffsbestimmung

Verstöße gegen diesen Vertrag sind insbesondere:

* Die Verarbeitung oder Nutzung der Datenbasis zu anderen als den Zwecken dieses Vertrags
* Keine oder unzureichende Angabe von Datenquellen in Veröffentlichungen
* Untersagte De-Anonymisierungen oder Re-Identifikationen von Personen
* Die unzulässige Zugänglichmachung der Datenbasis oder Derivate an Dritte
* Die Weitergabe von persönlichen Zugangscodes und Passwörtern
* Der Verlust von Datenträgern, die die Datenbasis oder Derivate enthalten
* Die Nichteinhaltung anderer im **Anhang Technische und organisatorische Maßnahmen** aufgelisteter Zusagen

#### Meldepflichten

Verstoßen Datennutzende gegen Verpflichtungen aus diesem Vertrag und insbesondere auch die Verpflichtung zur Einhaltung gesetzlicher Vorschriften, haben sie das FDZ unverzüglich zu informieren. Darüber hinaus ist das FDZ informieren, wenn eine gesetzliche Meldepflicht an die Datenschutzaufsichtsbehörden besteht.

#### Vertragsstrafen

###### Im Falle der Verletzung einer der in lit. a) genannten Verpflichtungen ergreift das FDZ je nach den Umständen und der Schwere des Falles eine oder mehrere der folgenden Maßnahmen:

* Die Datennutzenden haben die Datenbasis einschließlich etwaiger Derivate unverzüglich aus ihrem Bestand zu löschen;
* eine entsprechende Mitteilung über den Verstoß wird an die im Ständigen Ausschuss Forschungsdateninfrastruktur (FDI) versammelten Forschungsdatenzentren und den Rat für Sozial- und Wirtschaftsdaten (RatSWD) gesendet;
* die Datennutzende wird vorübergehend oder dauerhaft vom Zugang zu den Diensten und Leistungen des FDZ ausgeschlossen.

###### Für den Fall einer schuldhaften Zuwiderhandlung der Datennutzenden gegen die in diesem Vertrag beschriebenen Meldepflichten nach § 7 lit. b) ist eine vom FDZ nach billigem Ermessen festzusetzende, im Streitfall von der zuständigen Gerichtsbarkeit zu überprüfende, Vertragsstrafe an das FDZ zu zahlen. Bei der Bemessung der Höhe der Vertragsstrafe ist strafschärfend zu berücksichtigen, dass diese durch Einhaltung der Mitteilungspflichten hätte abgewendet werden können.

#### Fristlose Kündigung aus wichtigem Grund

Eine fristlose Kündigung aus wichtigem Grund kann insbesondere bei Vorliegen eines Vertragsverstoßes erfolgen.

#### Haftung

###### Die Datengebende Stelle und das FDZ haften gegenüber den Datennutzenden nicht für Verluste oder Schäden irgendwelcher Art im Zusammenhang mit den Vertragsdaten oder mit Schlussfolgerungen oder Empfehlungen, die in den übermittelten Daten enthalten sein können.

###### Das FDZ und die Datengebende Stelle haften nur für vorsätzliches oder grob fahrlässiges Handeln; die Haftung für Folgeschäden ist ausgeschlossen. Bei grob fahrlässigem Handeln wird die Haftung auf vorhersehbare Schäden beschränkt.

###### Der Haftungsausschluss und die Haftungsbeschränkung gelten nicht bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, bei Schäden aus der Verletzung wesentlicher Vertragspflichten (sog. Kardinalpflichten) sowie bei der Haftung für zugesicherte Eigenschaften. Bei der Verletzung von Kardinalpflichten wird die Haftung für leichte Fahrlässigkeit auf vorhersehbare Schäden beschränkt. Eine Haftung für die Eignung der Datensätze für den vom Datennehmer intendierten Zweck wird nicht übernommen. Die Datennutzenden erkennen hiermit an, dass sie für die Folgen der Maßnahmen, die sie aufgrund der erhaltenen Daten oder als Ergebnis ihrer Interpretation der erhaltenen Daten treffen, allein verantwortlich sind.

###### Die Datennutzenden haftet dem FDZ und dem Datengebenden Stelle für alle Schäden, die ihnen aus nicht vereinbarungsgemäßem Umgang (fahrlässig oder vorsätzlich) im Rahmen der Überlassung der Datenbasis entstehen und stellt sie insoweit von Haftungsansprüchen Dritter frei. Die Ersatzpflicht entfällt, soweit der Datenempfänger nachweisen kann, dass er die nach den Umständen des Falles gebotene Sorgfalt beachtet hat. Haftungsfälle berechtigen zur Kündigung aus wichtigem Grund. Die Geltendmachung weitergehender Ansprüche bleibt davon unberührt. Dies umfasst auch die Kosten einer angemessenen Rechtsverteidigung.

* 1. Sonstiges

#### Antikorruptionsklausel

Das FDZ ist berechtigt, den Vertrag fristlos zu kündigen, wenn die Datennutzenden, die für das FDZ mit der Vorbereitung, dem Abschluss oder der Durchführung dieses Vertrages befasst sind (einschließlich dem/der für das Projekt einzustellenden Wissenschaftler/in) oder ihnen nahe stehenden Personen, wozu insbesondere Angehörige im Sinne des § 11 Abs. 1 Nr. 1 des Strafgesetzbuches zählen, Geschenke oder sonstige Vorteile anbieten, verspricht oder gewährt. Solchen Handlungen des Antragstellers stehen Handlungen von Personen gleich, die von ihm beauftragt oder mit seinem Wissen und Willen für ihn tätig sind.

#### Änderungen/Teilunwirksamkeit

###### Änderungen dieses Vertrags sind nur gültig, wenn sie in Schriftform erfolgen; Anpassungen der Anhänge, wenn Sie in Textform erfolgen. Eine Partei kann von der anderen die Bestätigung der Änderung der Anhänge in Schriftform verlangen.

###### Sollte eine Bestimmung dieses Vertrags ungültig sein, so betrifft dies nicht den Vertrag als Ganzes. In einem solchen Falle ist der Vertrag seinem Sinn und Zweck entsprechend auszulegen, wobei zu berücksichtigen ist, was die Parteien gewollt hätten, wenn ihnen die Ungültigkeit einer Vertragsbestimmung bekannt gewesen wäre.

#### Anwendbares Recht

Es wird die Anwendung deutschen Rechts vereinbart. Ausschließlicher Gerichtsstand ist

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Hauptverantwortlich Datennutzende

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift FDZ

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Datengebende Stelle

**Anhänge**

# Anhang Technische- und organisatorische Maßnahmen

#### Anwendungsbereich

Die nachfolgenden technischen und organisatorischen Maßnahmen gelten, sofern nicht für einzelne Auftragsverarbeiter oder Datennutzende in Hinblick auf die in ihrem Verarbeitungsbereich andere Maßnahmen spezifiziert wurden.

#### Management

###### Eine dem Risiko der Datenbasis angemessene Organisationsstruktur für die Informationssicherheit ist vorhanden und in die Prozesse und Abläufe integriert.

###### ❑ Die konkrete Umsetzung der organisatorischen und technischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Voraussetzungen ist dem FDZ von den Datennutzenden durch ein Datensicherheitskonzept darzulegen.

###### Alle Datennutzenden sowie ggf. alle weiteren Personen, die mit der Datenbasis in Kontakt kommen sind angemessen geschult und kennen insbesondere auch die Pflichten aus diesem Vertrag.

###### ❑ Die Datennutzenden stellen sicher, dass zur Datenbasis sowie zu Derivaten nur Personen Zugang haben, die unter entsprechender Anwendung des Verpflichtungsgesetzes verpflichtet wurden.

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Anonymisierung, Pseudonymisierung und Datenminimierung

###### Die Datenbasis enthält …

❍ … unmittelbar personenbezogene

❍ … ausschließlich mindestens formal anonymisierte

❍ … ausschließlich mindestens faktisch anonymisierte

❍ … ausschließlich absolut anonymisierte

… Daten.

###### ❑ Die Daten sind pseudonymisiert, wobei der unmittelbare Personenbezug über eine abgetrennte Verknüpfungstabelle hergestellt werden kann. Der Personenbezug des verbleibenden Datenbestands, also die Datenbasis – ohne die Pseudonyme – ist im o.g. Sinne anonymisiert/personenbezogen.

###### Die Datennutzenden verpflichten sich im Rahmen nur diejenigen Daten der Datenbasis zu verarbeiten, die sie benötigen; soweit hierfür weitere Anonymisierungsmaßnahmen möglich sind, sind diese durchzuführen. So sind etwa auch auszugsweise Notizen – sofern zulässig – soweit wie möglich abstrahiert und anonymisiert darzustellen.

###### ❑ Die Datenbasis darf nicht – auch nicht auszugsweise – mit weiteren Daten auf Individualebene (etwa auf Ebene von Personen, Haushalten oder Institutionen) zusammengeführt werden. Für die Verknüpfung, das „Mergen“ oder die Ergänzung der Datenbasis durch externe Daten muss ein schriftlicher Antrag gestellt werden. Nach Genehmigung des Antrags erhalten die Datennutzenden ggf. eine Verknüpfungstabelle um die Verknüpfung selbst vorzunehmen. Antrag und Vorgehensweise sind zu dokumentieren und als **Anhang Verknüpfungen** zu diesem Vertrag zu nehmen.

###### Jede Handlung, die darauf abzielt oder geeignet ist, die in den qualitativen Daten enthaltenen anonymisierten Informationen über Personen oder Organisationen zu deanonymisieren, ist zu unterlassen.

###### Sollten in der Datenbasis enthaltene anonymisierte Daten – auch unbeabsichtigt – deanonymisiert werden oder sollten die Datennutzenden Möglichkeiten zur Deanonymisierung entdecken oder einen diesbezüglichen Verdacht haben, ist dies dem FDZ mitzuteilen. Dabei dürfen in der ersten Mitteilung keine für die Deanonymisierung verwendbaren und/oder sensiblen Informationen über Personen oder Organisationen schriftlich oder mündlich ohne vorherige Abstimmung genannt werden. Es ist zunächst ein sicherer Kommunikationskanal zur Absprache des möglichen weiteren Vorgehens – etwa in Hinblick auf Melde- und Benachrichtigungspflichten – zu vereinbaren.

❑ Die erste Mitteilung muss in schriftlicher Form erfolgen.

###### Deanonymisierte Daten sind auf Anweisung des FDZ zu löschen. Diese Anweisung soll in Textform erfolgen, die Durchführung ist in Textform zu bestätigen. Die Löschung nach Anweisung entbindet die Datennutzenden von der Darlegungslast bezüglich der Sachverhalte, die der Löschung unterlagen. Das FDZ ist verpflichtet, den Datennutzenden in behördlichen oder gerichtlichen Verfahren seine Dokumentation des Sachverhaltes zur Verfügung zu stellen.

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Verschlüsselung

###### ❑ Es erfolgt eine Verschlüsselung von mobilen Datenträgern (wie DVD, USB Sticks, Festplatte), die die Datenbasis oder ihre Derivate enthalten nach Stand der Technik.

###### ❑ Bei E-Mail, Messenger, Cloud-Plattformen erfolgt eine Transportverschlüsselung und eine Inhaltsverschlüsselung der Datenbasis und ihrer Derivate nach dem Stand der Technik. Bei Nutzung dieser Dienste ist durch die Art der Verschlüsselung sicher zu stellen, sodass auch der Dienstanbieter keine Entschlüsselung der Datenbasis oder ihrer Derivate vornehmen kann.

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Vertraulichkeit

###### ❑ Die Datennutzenden verpflichten sich auch in mündlichen Präsentationen oder Gesprächen mit Dritten keine personenbezogenen Informationen weiterzugeben, einschließlich solcher Informationen, die zur Re-Identifikation von Personen oder Organisationen führen können.

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Freigabe vor Veröffentlichung

###### ❑ Die Datennutzenden sind verpflichtet alle auf der Datenbasis beruhenden Veröffentlichungen mindestens \_\_\_\_\_\_\_\_ Wochen vor der geplanten Veröffentlichung zur Prüfung der Einhaltung dieser Vereinbarung vorzulegen. Die Datengebende Stelle soll – sofern sie keine Einwände hat – die Freigabe erteilen. Widerspricht sie innerhalb von \_\_\_\_\_\_\_\_ Wochen der Freigabe nicht, gilt die Freigabe als erteilt. Sofern die Datengebende Stelle der Veröffentlichung widerspricht, muss sie den Widerspruch begründen. Sie soll die Datennutzenden bei der Erstellung einer vertragskonformen Veröffentlichung unterstützen.

#### Verfügbarkeit

###### Die Datenbasis wird den Datennutzenden vom FDZ …

❑ zum Download (off-site-Nutzung)

❑ zur Einsichtnahme in einer geschützten Online-Umgebung (remote Desktop)

❑ zur Ausführung von Analyse und dessen Ergebnis im Rahmen einer kontrollierten Datenfernverarbeitung (remote Execution)

❑ zur Einsichtnahme in den Räumlichkeiten des FDZ (on-site Nutzung)

… verfügbar gemacht. Der Zugang ist näher im **Anhang Datenzugang** beschrieben.

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Regelmäßige Überprüfung

###### ❑ System- und Sicherheitstests wie z. B. Code-Scan und Penetrationstests, werden regelmäßig durchgeführt.

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Autorisierung

###### ❑ Verwendung von starken Passwörtern und Veröffentlichung einer Richtlinie dafür – z. B. mind. 10-tellig bei zufälligen komplexen Zeichen oder mind. 16-stellig bei einfacheren Zeichenfolgen ohne direkte Verwendung von üblichen Wörtern

###### ❑ Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden.

###### ❑ Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetze oder die IT-Abteilung) – im Ausnahmefall (z. B. längere Erkrankung) wird das Passwort durch die IT zurückgesetzt und dieser Vorgang dokumentiert.

###### ❑ Passwörter dürfen nicht auf Zettel oder Pinnwänden aufgezeichnet werden.

###### ❑ Keine Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort

###### ❑ Einsatz von Verfahren zur Zwei- oder Mehr-Faktor-Authentifizierung bei Verarbeitungstätigkeiten vor dem Zugriff auf die Datenbasis oder ihre Derivate (z. B. Chipkarten, Token)

###### ❑ weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### physischen Sicherheit

###### ❑ Es besteht ein umfassendes Gesamtkonzept zur Gebäudeabsicherung im Allgemeinen (z. B. Brandschutz, Zutrittsbeschränkung und -kontrolle).

###### ❑ Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz).

###### ❑ Es bestehen klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung, zuständige/r Mitarbeiter/in für Besucher/innen) als Bestandteil des Konzepts

###### ❑ Stabile, einbruchshemmende Fenster und Türen im EG (z. B. nach DIN EN 1627)

###### ❑ Einsatz von Alarmanlagen zur Einbruchserkennung, insbesondere außerhalb der Arbeitszeit

###### ❑ Einsatz von Sicherheitspersonal (ggf. extern)

###### ❑ Einsatz von Videoüberwachungssystemen unter Berücksichtigung datenschutzrechtlicher Anforderungen (Monitoring des Zugangsschutzes)

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Protokollierung

###### ❑ Zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Systemkonfiguration

###### ❑ Prüfung eingehender E-Mails mittels Anti-Malwareschutz und Blockieren von gefährlichen E-Mail-Anhängen (z. B. .exe)

###### ❑ Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung

###### ❑ Software und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen

###### ❑ Die Datenbasis darf nur im Browser rezipiert werden. Nach dem Ende des Zugriffs auf Dokumente dürfen auf dem Computer des Benutzers keine Rückstände mehr bestehen, dies betrifft ausdrücklich auch alle temporären Speicherungen oder Zwischenspeicherungen etwa durch den Browser. Der Browser-Cache ist nach der Nutzung zu löschen.

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Zertifizierung

###### ❑ Die Datennutzenden oder die von ihnen beauftragten Auftragsverarbeiter verfügen über eine Zertifizierung für ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001, deren genauer Anwendungsbereich dem beigefügten Anhang zu entnehmen ist.

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Speicherbegrenzung

###### ❑ Originaldatenträger sind zurück zu geben.

###### ❑ Auch Datensätze, die durch mathematische Veränderungen der gelieferten Daten entstanden, sind zu löschen (damit ebenfalls: Derivate der Datenbasis im Sinne des Vertrages). Die verwendeten die Auswertungsprogramme, -syntaxen und -algorithmen sind durch die Datennutzenden entsprechend guter wissenschaftlicher Praxis zu archivieren.

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Rechenschaftspflicht

###### Sicherheitsvorkommnisse werden konsequent dokumentiert und dem FDZ mitgeteilt.

###### ❑ Jede Erstellung von Kopien der Datenbasis (Derivate), die nicht nur temporär erstellt wird und mindestens am gleichen Arbeitstag gelöscht wird, ist durch den Datennutzenden zu dokumentieren (mindestens: Dateiname, Speicherort und -datum). Die Dokumentation ist dem FDZ auf Verlangen herauszugeben.

###### ❑ Die Löschung der Datenbasis und ihrer Derivate ist zu dokumentieren.

❑ Die Dokumentation ist dem FDZ auf Verlangen herauszugeben.

❑ Die Löschung der Datenbasis und der Derivate bei Ende der Nutzungsrechte ist dem FDZ durch jeden Datennutzenden zu bestätigen.

###### ❑ Auf Aufforderung einer anderen Vertragspartei haben die Datennutzenden die datenschutzrechtlichen Verpflichtung ihrer zugriffsberechtigten Mitarbeitenden nachzuweisen.

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Löschung

###### ❑ Die Löschung von Daten soll unter Beachtung der Vorgaben des BSI-Grundschutz-Kompendiums, CON.6: Löschen und Vernichten[[1]](#footnote-1) erfolgen. Insbesondere ist bei der Löschung sicher zu stellen, dass die Daten nicht nur als gelöscht markiert wurden sondern etwa durch Zufallswerte überschrieben wurden.

###### ❍ Für die Entsorgung und Vernichtung von Datenträgern und Papier ist DIN 66399 mindestens nach Klasse 2 (mindestens Sicherheitsstufe auf dem Niveau 3, i.e. P-3 für Papier[[2]](#footnote-2), H-3 für klassische Festplatten[[3]](#footnote-3)) einzuhalten.

❍ Für die Entsorgung und Vernichtung von Datenträgern und Papier ist DIN 66399 mindestens nach Klasse 2 (mindestens Sicherheitsstufe auf dem Niveau 3, i.e. P-4[[4]](#footnote-4) für Papier, H-4[[5]](#footnote-5) für klassische Festplatten, E-4 für SSDs) der DIN 66399 einzuhalten.

###### ❑ Weitere:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Anhang Datennutzende

|  |
| --- |
| ❍ Die Institution \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – Datennutzende – |

*(oder)*

|  |  |
| --- | --- |
| ❍ Die natürlichen Person  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ❑ - als Angehörige/r der Institution -  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – Datennutzende – | |

tritt dem Datennutzungsvertrag mit der Vertragsnummer/-bezeichnung: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

bei.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Datennutzende/r

# Anhang Datenbasis

|  |  |  |
| --- | --- | --- |
| Titel | Version | doi |
|  |  |  |
|  |  |  |
|  |  |  |

# Anhang Datenzugang

*Beispiele*

Die Datennehmenden erhalten die Datenbasis auf maschinenlesbaren, verschlüsselten Datenträgern in der Regel einen Monat nach Abschluss dieses Vertrags per Post an die im Vertrag angegebene Postanschrift. Das Passwort zur Entschlüsselung wird in getrenntem Schreiben zugestellt/per Nachricht an die angegebene Handynummer verschickt.

*oder*

Die Datenbasis wird online unter https://fdz.de nach vorheriger Anmeldung zur Verfügung gestellt; die Zugangsdaten hierfür werden per Post an die im Anhang Datennutzende Anschriften übermittelt.

# Anhang Kostenmodell

*Beispiele*

Für die Download-Datenübermittlung und die Dokumentation werden keine Kosten erhoben.

Für die postalische Zusendung der Datenbasis fällt eine Aufwandspauschale in Höhe von 30 Euro an.

# Anhang Vorhaben

*Beispiel*

Titel des Forschungsvorhabens

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Beginn des Vorhabens (Tag/Monat/Jahr)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ende des Vorhabens (Tag/Monat/Jahr)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Beschreibung des Forschungsvorhabens  
(Kurze Darstellung des Erkenntnisziels bzw. der zentralen Fragestellungen des Vorhabens)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Beschreibung des methodischen Ansatzes  
(Forschungsmethoden)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Qualifizierungsprojekt ☐ Ja ☐ Nein

☐ Bachelor/Master ☐ Promotion ☐ Habilitation

# Anhang Zitationsregeln

# Anhang EU-Standardvertragsklauseln

## ABSCHNITT I

Klausel 1 Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (1) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

**b**) Die Parteien:

##### i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und

##### ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“), haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) einverstanden erklärt.

c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.

d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2 Wirkung und Unabänderbarkeit der Klauseln

a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3 Drittbegünstigte

a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:

##### i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7

##### ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b

##### iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e

##### iv) Klausel 12 — Modul eins: Klausel 12 Buchstaben a und d Module zwei und drei: Klausel 12 Buchstaben a, d und f

##### v) Klausel 13

##### vi) Klausel 15.1 Buchstaben c, d und e

##### vii) Klausel 16 Buchstabe e

##### viii) Klausel 18 — Module eins, zwei und drei Klausel 18 Buchstaben a und b Modul vier: Klausel 18

b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4 Auslegung

a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6 Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7 — fakultativ Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und Anhang I.A unterzeichnet.

b) Nach Ausfüllen der Anlage und Unterzeichnung von Anhang I.A wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in Anhang I.A.

c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

## ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8 Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

8.1. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e) der Übermittlung. Er darf die personenbezogenen Daten nur dann für einen anderen Zweck verarbeiten,

i) wenn er die vorherige Einwilligung der betroffenen Person eingeholt hat,

ii) wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder

iii) wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.

8.2. Transparenz

a) Damit betroffene Personen ihre Rechte gemäß Klausel 10 wirksam ausüben können, teilt der Datenimporteur ihnen entweder direkt oder über den Datenexporteur Folgendes mit:

##### i) seinen Namen und seine Kontaktdaten,

##### ii) die Kategorien der verarbeiteten personenbezogenen Daten,

##### iii) das Recht auf Erhalt einer Kopie dieser Klauseln,

##### iv) wenn er eine Weiterübermittlung der personenbezogenen Daten an Dritte beabsichtigt, den Empfänger oder die Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), den Zweck und den Grund einer solchen Weiterübermittlung gemäß Klausel 8.7.

b) Buchstabe a findet keine Anwendung, wenn die betroffene Person bereits über die Informationen verfügt, einschließlich in dem Fall, wenn diese Informationen bereits vom Datenexporteur bereitgestellt wurden, oder wenn sich die Bereitstellung der Informationen als nicht möglich erweist oder einen unverhältnismäßigen Aufwand für den Datenimporteur mit sich bringen würde. Im letzteren Fall macht der Datenimporteur die Informationen, soweit möglich, öffentlich zugänglich.

c) Die Parteien stellen der betroffenen Person auf Anfrage eine Kopie dieser Klauseln, einschließlich der von ihnen ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, können die Parteien Teile des Textes der Anlage vor der Weitergabe einer Kopie unkenntlich machen; sie legen jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen.

d) Die Buchstaben a bis c gelten unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.3. Richtigkeit und Datenminimierung

a) Jede Partei stellt sicher, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Der Datenimporteur trifft alle angemessenen Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Hinblick auf den/die Zweck(e) der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

b) Stellt eine der Parteien fest, dass die von ihr übermittelten oder erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet sie unverzüglich die andere Partei.

c) Der Datenimporteur stellt sicher, dass die personenbezogenen Daten angemessen und erheblich sowie auf das für den/die Zweck(e) ihrer Verarbeitung notwendige Maß beschränkt sind.

8.4. Speicherbegrenzung

Der Datenimporteur speichert die personenbezogenen Daten nur so lange, wie es für den/die Zweck(e), für den/die sie verarbeitet werden, erforderlich ist. Er trifft geeignete technische oder organisatorische Maßnahmen, um die Einhaltung dieser Verpflichtung sicherzustellen; hierzu zählen auch die Löschung oder Anonymisierung (2) der Daten und aller Sicherungskopien am Ende der Speicherfrist.

8.5. Sicherheit der Verarbeitung

a) Der Datenimporteur und — während der Datenübermittlung — auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffene Person gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

b) Die Parteien haben sich auf die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen geeinigt. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

c) Der Datenimporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

d) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

e) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, meldet der Datenimporteur die Verletzung unverzüglich sowohl dem Datenexporteur als auch der gemäß Klausel 13 festgelegten zuständigen Aufsichtsbehörde. Diese Meldung enthält i) eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), ii) ihre wahrscheinlichen Folgen, iii) die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und iv) die Kontaktdaten einer Anlaufstelle, bei der weitere Informationen eingeholt werden können. Soweit es dem Datenimporteur nicht möglich ist, alle Informationen zur gleichen Zeit bereitzustellen, kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

f) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Datenimporteur ebenfalls die jeweiligen betroffenen Personen unverzüglich von der Verletzung des Schutzes personenbezogener Daten und der Art der Verletzung, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur, unter Angabe der unter Buchstabe e Ziffern ii bis iv genannten Informationen, es sei denn, der Datenimporteur hat Maßnahmen ergriffen, um das Risiko für die Rechte oder Freiheiten natürlicher Personen erheblich zu mindern, oder die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. Im letzteren Fall gibt der Datenimporteur stattdessen eine öffentliche Bekanntmachung heraus oder ergreift eine vergleichbare Maßnahme, um die Öffentlichkeit über die Verletzung des Schutzes personenbezogener Daten zu informieren.

g) Der Datenimporteur dokumentiert alle maßgeblichen Fakten im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, einschließlich ihrer Auswirkungen und etwaiger ergriffener Abhilfemaßnahmen, und führt Aufzeichnungen darüber.

8.6. Sensible Daten

Sofern die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Datenimporteur spezielle Beschränkungen und/oder zusätzliche Garantien an, die an die spezifische Art der Daten und die damit verbundenen Risiken angepasst sind. Dies kann die Beschränkung des Personals, das Zugriff auf die personenbezogenen Daten hat, zusätzliche Sicherheitsmaßnahmen (wie Pseudonymisierung) und/oder zusätzliche Beschränkungen in Bezug auf die weitere Offenlegung umfassen.

8.7. Weiterübermittlungen

Der Datenimporteur darf die personenbezogenen Daten nicht an Dritte weitergeben, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union (3) ansässig sind (im Folgenden „Weiterübermittlung“), es sei denn, der Dritte ist im Rahmen des betreffenden Moduls an diese Klauseln gebunden oder erklärt sich mit der Bindung daran einverstanden. Andernfalls ist eine Weiterübermittlung durch den Datenimporteur nur in folgenden Fällen zulässig:

i) Sie erfolgt an ein Land, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,

ii) der Dritte gewährleistet auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung,

iii) der Dritte geht mit dem Datenimporteur ein bindendes Instrument ein, mit dem das gleiche Datenschutzniveau wie gemäß diesen Klauseln gewährleistet wird, und der Datenimporteur stellt dem Datenexporteur eine Kopie dieser Garantien zur Verfügung,

iv) die Weiterübermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich,

v) die Weiterübermittlung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, oder

vi) – falls keine der anderen Bedingungen erfüllt ist — der Datenimporteur hat die ausdrückliche Einwilligung der betroffenen Person zu einer Weiterübermittlung in einem speziellen Fall eingeholt, nachdem er sie über den/die Zweck(e), die Identität des Empfängers und die ihr mangels geeigneter Datenschutzgarantien aus einer solchen Übermittlung möglicherweise erwachsenden Risiken informiert hat. In diesem Fall unterrichtet der Datenimporteur den Datenexporteur und übermittelt ihm auf dessen Verlangen eine Kopie der Informationen, die der betroffenen Person bereitgestellt wurden.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.8. Verarbeitung unter der Aufsicht des Datenimporteurs

Der Datenimporteur stellt sicher, dass jede ihm unterstellte Person, einschließlich eines Auftragsverarbeiters, diese Daten ausschließlich auf der Grundlage seiner Weisungen verarbeitet.

8.9. Dokumentation und Einhaltung der Klauseln

a) Jede Partei muss nachweisen können, dass sie ihre Pflichten gemäß diesen Klauseln erfüllt. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die unter seiner Verantwortung durchgeführten Verarbeitungstätigkeiten.

b) Der Datenimporteur stellt der zuständigen Aufsichtsbehörde diese Aufzeichnungen auf Verlangen zur Verfügung.

Klausel 9 Einsatz von Unterauftragsverarbeitern

Klausel nicht anwendbar im Kontext Verantwortlicher-Verantwortlicher

Klausel 10 Rechte betroffener Personen

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

a) Der Datenimporteur bearbeitet, gegebenenfalls mit Unterstützung des Datenexporteurs, alle Anfragen und Anträge einer betroffenen Person im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte gemäß diesen Klauseln unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang der Anfrage oder des Antrags. (10) Der Datenimporteur trifft geeignete Maßnahmen, um solche Anfragen und Anträge und die Ausübung der Rechte betroffener Personen zu erleichtern. Alle Informationen, die der betroffenen Person zur Verfügung gestellt werden, müssen in verständlicher und leicht zugänglicher Form vorliegen und in einer klaren und einfachen Sprache abgefasst sein.

b) Insbesondere unternimmt der Datenimporteur auf Antrag der betroffenen Person folgende Handlungen, wobei der betroffenen Person keine Kosten entstehen:

##### i) Er legt der betroffenen Person eine Bestätigung darüber vor, ob sie betreffende personenbezogene Daten verarbeitet werden, und, falls dies der Fall ist, stellt er ihr eine Kopie der sie betreffenden Daten und die in Anhang I enthaltenen Informationen zur Verfügung; er stellt, falls personenbezogene Daten weiterübermittelt wurden oder werden, Informationen über die Empfänger oder Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), an die die personenbezogenen Daten weiterübermittelt wurden oder werden, sowie über den Zweck dieser Weiterübermittlung und deren Grund gemäß Klausel 8.7 bereit; er informiert die betroffene Person über ihr Recht, gemäß Klausel 12 Buchstabe c Ziffer i bei einer Aufsichtsbehörde Beschwerde einzulegen;

##### ii) er berichtigt unrichtige oder unvollständige Daten über die betroffene Person;

##### iii) er löscht personenbezogene Daten, die sich auf die betroffene Person beziehen, wenn diese Daten unter Verstoß gegen eine dieser Klauseln, die Rechte als Drittbegünstigte gewährleisten, verarbeitet werden oder wurden oder wenn die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützt, widerruft.

c) Verarbeitet der Datenimporteur die personenbezogenen Daten für Zwecke der Direktwerbung, so stellt er die Verarbeitung für diese Zwecke ein, wenn die betroffene Person Widerspruch dagegen einlegt.

d) Der Datenimporteur trifft keine Entscheidung, die ausschließlich auf der automatisierten Verarbeitung der übermittelten personenbezogenen Daten beruht (im Folgenden „automatisierte Entscheidung“), welche rechtliche Wirkung für die betroffene Person entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen würde, es sei denn, die betroffene Person hat hierzu ihre ausdrückliche Einwilligung gegeben oder eine solche Verarbeitung ist nach den Rechtsvorschriften des Bestimmungslandes zulässig und in diesen sind angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person festgelegt. In diesem Fall muss der Datenimporteur, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur,

##### i) die betroffene Person über die geplante automatisierte Entscheidung, die angestrebten Auswirkungen und die damit verbundene Logik unterrichten und

##### ii) geeignete Garantien umsetzen, die mindestens bewirken, dass die betroffene Person die Entscheidung anfechten, ihren Standpunkt darlegen und eine Überprüfung durch einen Menschen erwirken kann.

e) Bei exzessiven Anträgen einer betroffenen Person — insbesondere im Fall von häufiger Wiederholung — kann der Datenimporteur entweder eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten für die Erledigung des Antrags verlangen oder sich weigern, aufgrund des Antrags tätig zu werden.

f) Der Datenimporteur kann den Antrag einer betroffenen Person ablehnen, wenn eine solche Ablehnung nach den Rechtsvorschriften des Bestimmungslandes zulässig und in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele zu schützen.

g) Beabsichtigt der Datenimporteur, den Antrag einer betroffenen Person abzulehnen, so unterrichtet er die betroffene Person über die Gründe für die Ablehnung und über die Möglichkeit, Beschwerde bei der zuständigen Aufsichtsbehörde einzulegen und/oder einen gerichtlichen Rechtsbehelf einzulegen.

Klausel 11 Rechtsbehelf

Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,

i) eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,

ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.

d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.

e) Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.

f) Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12 Haftung

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

b) Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.

c) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

d) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe c haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

e) Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

Klausel 13 Aufsicht

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

a) [Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

## ABSCHNITT III — LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14 Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

##### i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

##### ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien, (12)

##### iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht. [In Bezug auf Modul drei: Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.]

f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen, [in Bezug auf Modul drei: gegebenenfalls in Absprache mit dem Verantwortlichen]. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er [in Bezug Modul drei: vom Verantwortlichen oder] von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 15 Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

15.1. Benachrichtigung

a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,

##### i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

##### ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.). [In Bezug auf Modul drei: Der Datenexporteur leitet die Informationen an den Verantwortlichen weiter.]

d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

e) Die Buchstaben a bis c gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2. Überprüfung der Rechtmäßigkeit und Datenminimierung

a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14 Buchstabe e.

b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung. [In Bezug auf Modul drei: Der Datenexporteur stellt die Beurteilung dem Verantwortlichen zur Verfügung.]

c) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

## ABSCHNITT IV — SCHLUSSBESTIMMUNGEN

Klausel 16 Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.

c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

##### i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

##### ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

##### iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde [in Bezug auf Modul drei: und den Verantwortlichen] über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

d) [In Bezug auf die Module eins, zwei und drei: Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten.] [In Bezug auf Modul vier: Von dem in der EU ansässigen Datenexporteur erhobene personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen unverzüglich vollständig gelöscht werden, einschließlich aller Kopien.] Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17 Anwendbares Recht

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

[OPTION 1: Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von der Bundesrepublik Deutschland ist.]

Klausel 18 Gerichtsstand und Zuständigkeit

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

b) Die Parteien vereinbaren, dass dies die Gerichte von Deutschland sind.

c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.

d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

(1) Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

(2) Die Daten müssen in einer Weise anonymisiert werden, dass eine Person im Einklang mit Erwägungsgrund 26 der Verordnung (EU) 2016/679 nicht mehr identifizierbar ist; außerdem muss dieser Vorgang unumkehrbar sein.

(3) Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

(6) Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

(10) Diese Frist kann um höchstens zwei weitere Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Datenimporteur unterrichtet die betroffene Person ordnungsgemäß und unverzüglich über eine solche Verlängerung.

(12) Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. Dies betrifft insbesondere interne Aufzeichnungen oder sonstige Belege, die fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden, sofern diese Informationen rechtmäßig an Dritte weitergegeben werden können. Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden; den Parteien obliegt die sorgfältige Prüfung, ob alle diese Elemente ausreichend zuverlässig und repräsentativ sind, um die getroffene Schlussfolgerung zu bekräftigen. Insbesondere müssen die Parteien berücksichtigen, ob ihre praktische Erfahrung durch öffentlich verfügbare oder anderweitig zugängliche zuverlässige Informationen über das Vorhandensein oder Nicht-Vorhandensein von Ersuchen innerhalb desselben Wirtschaftszweigs und/oder über die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsgremien, erhärtet und nicht widerlegt wird.

## ANHANG I

A. LISTE DER PARTEIEN

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

Datenexporteur(e): [Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union]

1. Name: …

Anschrift: …

Name, Funktion und Kontaktdaten der Kontaktperson: …

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: …

Unterschrift und Datum: …

Rolle (Verantwortlicher/Auftragsverarbeiter): …

2. …

Datenimporteur(e): [Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson]

1. Name: …

Anschrift: …

Name, Funktion und Kontaktdaten der Kontaktperson: …

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: …

Unterschrift und Datum: …

Rolle (Verantwortlicher/Auftragsverarbeiter): …

2. …

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

…

Kategorien der übermittelten personenbezogenen Daten

…

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten,

Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

…

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)

…

Art der Verarbeitung

…

Zweck(e) der Datenübermittlung und Weiterverarbeitung

…

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

…

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

…

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

…

## ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret (nicht allgemein) beschrieben werden. Beachten Sie hierzu bitte auch die allgemeine Erläuterung auf der ersten Seite der Anlage; insbesondere ist klar anzugeben, welche Maßnahmen für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen gelten.

Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen

[Beispiele für mögliche Maßnahmen:

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Maßnahmen zum Schutz der Daten während der Übermittlung

Maßnahmen zum Schutz der Daten während der Speicherung

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Maßnahmen zur Gewährleistung der Datenminimierung

Maßnahmen zur Gewährleistung der Datenqualität

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.

## ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss für die Module zwei und drei im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 9 Buchstabe a, Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: …

Anschrift: …

Name, Funktion und Kontaktdaten der Kontaktperson: …

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): …

2. …

# Anhang Auftragsverarbeitungen

*Beispiel*

Die Datennutzenden setzen folgende Stellen im Wege der Auftragsverarbeitung ein:

Stelle (Bezeichnung und ladungsfähige Anschrift):

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Kurze Beschreibung des Gegenstands der Auftragsvereinbarung

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

❑ Die Auftragsvereinbarung nebst der Dokumentation der bei ihr eingesetzten technischen und organisatorischen Maßnahmen liegt anbei.

Oder

|  |  |
| --- | --- |
| Auftragsverarbeitende/r | Gegenstand |
|  |  |
|  |  |
|  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Hauptverantwortlich Datennutzende

❑ auch in Vertretung für bereits einbezogene Datennutzende

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift FDZ

❑ auch in Vertretung für die Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschriften weiterer Vertragsparteien

# Anhang Spezifische Einschränkungen der Verarbeitung

# Anhang Löschbestätigung

Hiermit bestätigt der/die/das

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

❑ vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

– Datennutzende/r –

dass sämtliche Daten (Datenbasis und Derivate),

die dem/der Datennutzenden im Rahmen des Datennutzungsvertrages mit der Vertragsnummer/-bezeichnung:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zwischen dem/der vorbezeichneten/r Datennutzenden/r und dem Forschungsdatenzentrum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

sowie ggf. weiteren Vertragsparteien

zur Verfügung gestellt wurden, entsprechend dem Datennutzungsvertrag zum Ende der Vertragslaufzeit von allen Rechnern, Servern und Datenträgern sicher und vollständig gelöscht wurden.

Dies schließt alle mir bereitgestellten Versionen der Datensätze ein. Auch alle Sicherungskopien, Auszugs- und Hilfsdateien sowie durch Weiterverarbeitung entstandene Datensätze wurden entsprechend gelöscht.

❑ Falls Sicherungskopien aus technischen oder organisatorischen Gründen nicht vernichtet werden können, versichere ich hiermit, dass ein Zurückspielen der Daten jederzeit ausgeschlossen ist.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Datennutzende

# Vertragserweiterung: Vertragsverlängerung

Der Datennutzungsvertrag mit der Vertragsnummer/-bezeichnung: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zwischen dem Forschungsdatenzentrum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

vertreten durch: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

und dem Hauptverantwortlich Datennutzenden

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

❑ vertreten durch: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

und etwaigen weiteren im vorgenannten Vertrag bezeichneten Parteien

wird bis zum \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ verlängert.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Hauptverantwortlich Datennutzende

❑ auch in Vertretung für einbezogene Datennutzende

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift FDZ

❑ auch in Vertretung für die Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Unterschrift Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschriften weiterer Vertragsparteien

# Vertragserweiterung: Datenbasis

Der Datennutzungsvertrag mit der Vertragsnummer/-bezeichnung: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zwischen dem Forschungsdatenzentrum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

vertreten durch: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

und dem Hauptverantwortlich Datennutzenden

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

❑ vertreten durch: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

und etwaigen weiteren im vorgenannten Vertrag bezeichneten Parteien als (einfache/r) Datennutzende/r beifolgende Datenbestände als Datenbasis des Vertrages. Die Vertragsbedingungen sind dem/der Beitretenden bekannt.

|  |  |  |
| --- | --- | --- |
| Titel | Version | doi |
|  |  |  |
|  |  |  |
|  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Hauptverantwortlich Datennutzende

❑ auch in Vertretung für bereits einbezogene Datennutzende

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift FDZ

❑ auch in Vertretung für die Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Unterschrift Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschriften weiterer Vertragsparteien

# Vertragserweiterung: Datennutzende

|  |
| --- |
| ❍ Die Institution \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – Datennutzende – |

*(oder)*

|  |  |
| --- | --- |
| ❍ Die natürlichen Person  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ❑ - als Angehörige/r der Institution -  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Anschrift:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – Datennutzende – | |

tritt dem Datennutzungsvertrag mit der Vertragsnummer/-bezeichnung: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zwischen

|  |
| --- |
| ❍ der Institution \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – Datengebende Stelle –  – gleichzeitig Forschungsdatenzentrum (FDZ) – |

*(oder)*

|  |  |
| --- | --- |
| ❍ der Institution  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – nachfolgend: Datengebende Stelle – | unter Vermittlung durch    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch  \_\_\_\_\_\_\_\_\_\_\_\_\_­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – Forschungsdatenzentrum (FDZ) – |

*(oder)*

|  |  |
| --- | --- |
| ❍ der natürlichen Person  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ❑ und als Angehörige/r der Institution  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – nachfolgend: Datengebende Stelle – | |
| unter Vermittlung durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – Forschungsdatenzentrum (FDZ) – | |

und dem Hauptverantwortlich Datennutzenden

|  |
| --- |
| ❍ der Institution \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Vertreten durch \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  – Hauptverantwortlich Datennutzende/r – |

*(oder)*

|  |  |
| --- | --- |
| ❍ der natürlichen Person  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ❑ und als Angehörige/r der Institution  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – Hauptverantwortlich Datennutzende/r – | |

und etwaigen weiteren im vorgenannten Vertrag bezeichneten Parteien als (einfache/r) Datennutzende/r bei. Die Vertragsbedingungen sind dem/der Beitretenden bekannt.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift beitretende/r Datennutzende/r

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift Hauptverantwortlich Datennutzende

❑ auch in Vertretung für bereits einbezogene Datennutzende

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum Unterschrift FDZ

❑ auch in Vertretung für die Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Unterschrift Datengebende Stelle

❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Unterschriften weiterer Vertragsparteien

1. Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg): IT-Grundschutz-Kompendium, Stand: Februar 2021, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2021.pdf>. [↑](#footnote-ref-1)
2. Fläche der Materialteilchen max. 320 mm2 oder Breite des Streifens max. 2 mm Streifenlänge unbegrenzt. [↑](#footnote-ref-2)
3. Datenträger verformt. [↑](#footnote-ref-3)
4. Fläche der Materialteilchen max. 160 mm2 und Breite des Streifens max. 6 mm. [↑](#footnote-ref-4)
5. Datenträger mehrfach zerteilt und verformt und Fläche der Materialteilchen max. 2000 mm2. [↑](#footnote-ref-5)