***Hinweis:*** Mit diesem Vertragsmuster können die erforderlichen Regelungen zur Datenverarbeitung im Auftrag gemäß Art. 28 DSGVO getroffen werden. Die Details der jeweiligen Verarbeitung und Beauftragung sind in den Anhängen 1 bis 6 festzulegen. (Die grün hinterlegten Felder müssen ausgefüllt werden, die weiteren Angaben wenn zutreffend.) Der Vertragstext selbst darf nicht verändert werden bzw. muss bei jeglichen Veränderungen neu vom Justitiariat geprüft werden.

Mustervertrag V3.1 (fernwartung), 30.07.2019 auf Basis ZENDAS Version 4.6, 09.04.2019

Muster-Vertrag zur
Datenverarbeitung im Auftrag
(Auftragsverarbeitung – AV)

Zwischen

der Hochschule x, Universitätsstr. 1, 12345 Hochschulstadt ,

vertreten durch die Kanzlerin Frau Dr. …/ die Rektorin Frau Prof. …

**− Verantwortlicher −**

und

der Firma ABC GmbH, Straße, Ort,

vertreten durch die Vertretungsberechtigte …

**− Auftragsverarbeiter −**

# Gegenstand und Dauer, Vergütung, Vorrang dieses Vertrags, Begrifflichkeit

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen.
2. Der Gegenstand der Verarbeitung und ein ggf. zugrundeliegender Vertrag werden im Anhang 2 dargestellt.
3. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem zugrundeliegenden Vertrag im Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden
4. Die Laufzeit dieser Vereinbarung richtet sich nach den Regelungen des der Auftragserteilung zugrundeliegenden Vertrags. Die vorliegende Vereinbarung bleibt gegebenenfalls darüber hinaus so lange gültig bis eine Löschung oder Übergabe nach § 5 Abs. 13 erfüllt ist.
5. Der Verantwortliche ist zu einer außerordentlichen Kündigung dieses Vertrags und des der Auftragserteilung zugrundeliegenden Vertrags berechtigt, wenn der Auftragsverarbeiter − soweit gesetzlich vorgeschrieben: trotz schriftlicher Aufforderung − die vereinbarten Leistungen nicht ordnungsgemäß erbringt oder Pflichten aus diesem Vertrag, insbesondere nach § 4, verletzt.
6. Eine gesonderte Vergütung erfolgt nicht, es sei denn, dies wird ausdrücklich vereinbart.
7. Soweit dieser Vertrag von dem der Auftragserteilung zugrundeliegenden Vertrag abweichende Regelungen trifft, gehen die Regelungen des Vertrags zur Datenverarbeitung im Auftrag vor.
8. Die datenschutzrechtliche Terminologie dieser Vereinbarung entspricht der der Datenschutz-Grund­ver­ord­nung (DSGVO) vom 27.04.2016.

# Konkretisierung des Auftragsinhalts hinsichtlich der Art und des Zwecks der Datenverarbeitung, der Art der personenbezogenen Daten und der Kategorien betroffener Personen

1. Art und Zweck der Datenverarbeitung durch den Auftragsverarbeiter für den Verantwortlichen sowie Art der verwendeten Daten und Kategorien der durch die Datenverarbeitung im Rahmen des Auftrags betroffenen Personen werden im Anhang 2 beschrieben.
2. Jede Verlagerung der Datenverarbeitung in einen Staat außerhalb der Europäischen Union (Drittland) bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind. Der Auftragsverarbeiter macht dazu Angaben im Anhang 1.

# Fernwartung

1. Die Regelungen dieses Paragraphen finden bei räumlich getrennten Zugriffen des Auftragsverarbeiters auf IT-Systeme des Verantwortlichen zu Wartungs- oder Reparaturzwecken (Fernwartung) Anwendung.
2. Der Auftragsverarbeiter darf im Rahmen der Fernwartung nur auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Fernwartung erforderlich ist. Ferner ist dem Auftragsverarbeiter bei der Fernwartung untersagt, personenbezogene Daten des Verantwortlichen auf eigenen IT-Systemen bzw. Datenträgern zu speichern, es sei denn der Verantwortliche weist ihn hierzu an.
3. Der Auftragsverarbeiter hat dem Verantwortlichen Fernwartungsarbeiten im Vorfeld anzukündigen. Der Verantwortliche ist berechtigt, die Durchführung der Fernwartung mit zu verfolgen bzw. Aufzeichnungen (z. B. Screenrecording, Screenshots o. Ä.) von dieser zu erstellen. Auf Anfrage und soweit erforderlich, wirkt der Auftragsverarbeiter an der Konfiguration technischer Kontrolleinrichtungen mit.
4. Im Rahmen der beauftragten und zu leistenden Fernwartungsarbeiten hat der Auftragsverarbeiter folgende Rahmenbedingungen bei Zugriff auf das Netzwerk, die IT-Systeme und Anwendungen des Verantwortlichen zu beachten:
* Der Auftragsverarbeiter erhält für Arbeiten an den IT-Systemen und Anwendungen personalisierte Benutzerkennungen. Jeder Mitarbeiter des Auftragsverarbeiters erhält eine eigene personalisierte Benutzerkennung. Der Auftragsverarbeiter nutzt die ihm überlassenen personalisierten Benutzerkennungen ausschließlich für die beauftragten Tätigkeiten und gibt diese nicht an Dritte weiter. Die Kennwortrichtlinien des Verantwortlichen sind einzuhalten.
* Nutzt der Auftragsverarbeiter für die Ausübung seiner Tätigkeiten eigene technische Geräte stellt er durch adäquate und dem Stand der Technik entsprechende, angemessene Maßnahmen sicher, dass von diesen keine Gefahren für die Netzinfrastruktur, IT-Systeme und Anwendungen des Verantwortlichen ausgehen.
* Änderungen an den IT-Systemen und Anwendungen seitens des Auftragsverarbeiters sind mit dem Verantwortlichen abzustimmen und in einem adäquaten, prüffähigen Umfang zu dokumentieren.
1. Insbesondere beim Fernzugriff auf das Netzwerk und die IT-Systeme des Verantwortlichen gelten die zusätzlichen Bedingungen:
* Das Netz und die für die Fernwartung genutzten IT-Systeme des Auftragsverarbeiters müssen adäquat gegen unberechtigte Zugriffe geschützt sein.
* Der Fernzugriff auf das Netzwerk des Verantwortlichen erfolgt ausschließlich über eine nach dem Stand der Technik angemessen sichere, verschlüsselte Verbindung.
* Der Fernzugriff sollte generell nur innerhalb der üblichen Arbeitszeiten des Verantwortlichen durchgeführt werden. Ein Fernzugriff außerhalb dieser Zeiten ist mit dem Verantwortlichen abzustimmen und zu dokumentieren.
* Der Zugriff ist nach erfolgter Tätigkeit zu beenden und die Verbindung zu schließen.
* Die erfolgten Zugriffe werden vom Auftragsverarbeiter wie in Anhang 5 vereinbart protokolliert.

# Weisungs- und Kontrollrechte

1. Der Verantwortliche bleibt für die Einhaltung der Vorschriften über den Datenschutz, insbesondere der DSGVO sowie des DSG-NRW, verantwortlich.
2. Der Verantwortliche hat das Recht, dem Auftragsverarbeiter Weisungen zu erteilen hinsichtlich der Verarbeitung der personenbezogenen Daten. Diese sind zu dokumentieren.
3. Weisungsberechtigte Personen auf Seiten des Verantwortlichen sowie Weisungsempfänger auf Seiten des Auftragsverarbeiters werden im Anhang 3 festgelegt.
4. Bei einem Wechsel oder einer längerfristigen Verhinderung einer der im Anhang 3 aufgeführten Personen ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.
5. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder des nationalen Rechts verstößt.
6. Weisungen, die die unter § 1 und § 2 dieses Vertrags getroffenen Festlegungen ändern, aufheben oder ergänzen, sind nur zulässig, wenn eine entsprechende neue schriftliche Festlegung erfolgt.
7. Der Verantwortliche ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und die vertraglichen Vereinbarungen im Rahmen des Auftragsverhältnisses im erforderlichen Umfang zu kontrollieren oder durch eine von ihm beauftragte Person kontrollieren zu lassen, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme im Rahmen von Inspektionen. Der Auftragsverarbeiter unterstützt die Kontrollen. Er verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

# Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern der Auftragsverarbeiter nicht durch das Recht der Europäischen Union oder des nationalen Rechts, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. Eine Verarbeitung zu anderen Zwecken ist ausgeschlossen. Der Auftragsverarbeiter hat personenbezogene Daten zu berichtigen, zu löschen und einzuschränken, wenn der Verantwortliche dies in der getroffenen Vereinbarung oder in einer Weisung verlangt.
3. Der Auftragsverarbeiter sichert im Rahmen des Auftragsverhältnisses die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.
4. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erstellung und Führung des Verzeichnisses über die Verarbeitungstätigkeiten, insbesondere durch Mitteilung der erforderlichen Angaben.
5. Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
6. Sofern sich Daten des Verantwortlichen auf Datenträgern des Auftragsverarbeiters befinden, wird folgendes vereinbart:
	1. Eignen sich die Datenträger zur Übergabe, übereignet der Auftragsverarbeiter dem Verantwortlichen zur Sicherung diese Datenträger. Diese Datenträger sind besonders zu kennzeichnen. Der Auftragsverarbeiter verpflichtet sich, mindestens einen Datenträger vorzuhalten, auf dem alle Daten des Verantwortlichen gespeichert werden können und der übereignet werden kann. Der Auftragsverarbeiter verwahrt den Datenträger bis zur Herausgabe an den Verantwortlichen für diesen unentgeltlich.
	2. Eignen sich die Datenträger nicht zur Übergabe, verpflichtet sich der Auftragsverarbeiter in dem Fall, in dem aufgrund von Maßnahmen Dritter (etwa bei Pfändung), bei Insolvenz- oder Vergleichsverfahren oder bei sonstigen Ereignissen die Gefahr besteht, dass diese Daten in die Hände Dritter gelangen, sie auf den Datenträger nach Absatz 6 lit. a Satz 3 zu kopieren und diese Daten auf den von der Maßnahme Dritter bzw. von den Ereignissen betroffenen Datenträgern datenschutzgerecht zu löschen.
7. Sollte das Eigentum oder die Vertraulichkeit der Daten des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung), durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren.
8. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, Verdacht auf Verletzungen des Schutzes personenbezogener Daten, anderen Unregelmäßigkeiten bei der Datenverarbeitung, bei Kontrollhandlungen und Maßnahmen einer Aufsichts- oder Ermittlungsbehörde. Der Auftragsverarbeiter benachrichtigt unverzüglich den Verantwortlichen, wenn die bei ihm getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht (mehr) genügen.
9. Im Falle einer Verletzung des Schutzes personenbezogener Daten ergreift der Auftragsverarbeiter im Benehmen mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für betroffene Personen. Er unterstützt den Verantwortlichen bei der Erfüllung von datenschutzrechtlichen Meldepflichten gegenüber der Aufsichtsbehörde und Benachrichtigungspflicht gegenüber betroffenen Personen.
10. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen beim Treffen der erforderlichen technischen und organisatorischen Maßnahmen, insbesondere nach Art. 32 DSGVO.
11. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Durchführung einer ggf. notwendigen Untersuchung der Auswirkung der Verarbeitung auf die ‚Rechte und Freiheiten natürlicher Personen, insbesondere im Falle einer gemäß Art. 35 DSGVO erforderlichen Datenschutzfolgeabschätzung sowie bei Vorliegen der Voraussetzungen des Art. 36 Abs. 1 DSGVO bei der vorherigen Konsultation der Aufsichtsbehörden.
12. Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung dabei nach Möglichkeit, mit geeigneten technischen und organisatorischen Maßnahmen, seiner Pflicht zur Beantwortung von Anträgen einer betroffenen Person auf Wahrnehmung ihrer in Kapitel III der DSGVO genannten Rechte nachzukommen (wie transparente Informationen, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung).
13. Der Auftragsverarbeiter hat dem Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen datenschutzgerecht zu löschen oder zurückzugeben, sofern nicht nach dem Recht der Europäischen Union oder dem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dem Verantwortlichen ist auf Verlangen ein Nachweis über die Löschung vorzulegen. Ein Zurückbehaltungsrecht wird hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.

# Unterauftragsverhältnisse

1. Der Verantwortliche stimmt dem Einsatz der im Anhang 4 genannten weiteren Auftragsverarbeitern (Unterauftragnehmer) zu. Dort ist ebenfalls geregelt, wie ggf. mit einem geplanten Einsatz von weiteren Auftragsverarbeitern durch den Auftragsverarbeiter verfahren werden soll.
2. Bei der Beauftragung eines weiteren Auftragsverarbeiters stellt der Auftragsverarbeiter vertraglich sicher, dass die in diesem Vertrag vereinbarten Regelungen (insbesondere die Prüf- und Kontrollrechte des Verantwortlichen) auch gegenüber dem weiteren Auftragsverarbeiter gelten. Auch müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen insbesondere der DSGVO erfolgt. Der Auftragsverarbeiter weist dies dem Verantwortlichen nach. Der Auftragsverarbeiter hat die Einhaltungen der Regelungen durch den von ihm beauftragten weiteren Auftragsverarbeiter regelmäßig zu überprüfen.
3. Kommt ein weiterer Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Pflichten jenes anderen Auftragsverarbeiters.
4. Der Auftragsverarbeiter teilt dem Verantwortlichen die für das Verzeichnis der Verarbeitungstätigkeiten erforderlichen Informationen zur Datenverarbeitung durch den weiteren Auftragsverarbeiter mit.
5. Die Weiterleitung von Daten an einen weiteren Auftragsverarbeiter ist erst zulässig, wenn alle Voraussetzungen für eine Unterbeauftragung vorliegen.

# Vertraulichkeit, Datengeheimnis, Datenschutzbeauftragter

1. Jede Partei ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Vertragspartners vertraulich zu behandeln. Diese Pflicht besteht auch nach Vertragsende fort.
2. Die Pflicht zur Vertraulichkeit besteht nicht, wenn die vertrauliche Information bereits öffentlich bekannt war, als sie dem jeweils anderen Vertragspartner mitgeteilt wurde, öffentlich wird, nachdem sie dem jeweils anderen Vertragspartner mitgeteilt wurde und die Veröffentlichung nicht unter Verletzung vertraglicher oder gesetzlicher Bestimmungen erfolgte, der jeweils andere Vertragspartner auf die Vertraulichkeit verzichtet oder aufgrund behördlicher oder gesetzlicher Anordnung eine Mitteilung an Dritte angeordnet wird .
3. Der Vertragspartner, der sich auf eine der vorgenannten Ausnahmen beruft, trägt die Beweislast dafür, dass der Ausnahmetatbestand, auf den er sich beruft, erfüllt ist.
4. Den zur Verarbeitung der personenbezogenen Daten befugten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Der Auftragsverarbeiter gewährleistet, dass sich diese Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Etwaige Verpflichtungserklärungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Auftragsverarbeiter und den bei ihm beschäftigten Personen bestehen bleiben. Dem Verantwortlichen sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.
5. Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften, insbesondere der DSGVO, des DSG-NRW, BDSG und des Strafgesetzbuchs, bekannt sind, und sichert zu, dass er die bei der Durchführung der Arbeiten Beschäftigten mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
6. Der Auftragsverarbeiter darf Auskünfte an Dritte oder betroffene Personen nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Ist der Auftragsverarbeiter gerichtlich oder gesetzlich verpflichtet, Auskunft zu erteilen, so hat er den Verantwortlichen hierüber unverzüglich zu informieren. Der Auftragsverarbeiter darf Auskünfte an den Verantwortlichen nur gegenüber den autorisierten Personen (gemäß Anhang 3) erteilen.
7. Ist der Auftragsverarbeiter gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet, so ist dieser vor Beginn der Vertragsdurchführung zu bestellen. Der Auftragsverarbeiter teilt dem Verantwortlichen dessen Kontaktdaten mit und trägt diese in Anhang 1 ein. Entsprechendes gilt bei einem Wechsel in der Person des Datenschutzbeauftragten.

# Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter erstellt ohne Wissen des Verantwortlichen keine Kopien oder Duplikate der im Auftrag verarbeiteten Daten.
2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich in seinen Geschäftsräumen. Ausnahmen hiervon, z. B. im Rahmen von Heim- oder Telearbeit, sind nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen zulässig.
3. Der Auftragsverarbeiter hat Test- und Ausschussmaterial unverzüglich datenschutzgerecht zu vernichten oder dem Verantwortlichen auszuhändigen. Die Löschung bzw. Vernichtung ist dem Verantwortlichen mit Datumsangabe schriftlich zu bestätigen.
4. Der Auftragsverarbeiter sichert zu, dass die verarbeiteten Daten des Verantwortlichen von sonstigen Datenbeständen getrennt werden.
5. Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO zur Sicherheit der Verarbeitung erforderlichen Maßnahmen und macht dazu Angaben im Anhang 6.
6. Die im Anhang 6 vereinbarten technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Änderungen und Ergänzungen der vereinbarten technischen und organisatorischen Maßnahmen bedürfen einer schriftlichen Mitteilung an die weisungsberechtigte(n) Person(n) des Verantwortlichen und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Maßnahmen handelt. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen bedürfen der Zustimmung des Verantwortlichen. Bei allen Änderungen der technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter darf das Sicherheitsniveau der vereinbarten Maßnahmen nicht unterschritten werden.

# Haftung

1. Ist der Verantwortliche zum Schadensersatz gegenüber der betroffenen Person verpflichtet, so stellt der Auftragsverarbeiter den Verantwortlichen von der Haftung frei, soweit der Auftragsverarbeiter oder ein weiterer Auftragsverarbeiter den Schaden schuldhaft herbeigeführt hat.
2. Im Übrigen gelten für die Haftung die Regelungen des dieser Vereinbarung zugrundeliegenden Vertragsverhältnisses.

# Sonstiges

1. Änderungen, Ergänzungen und Nebenabreden dieses Vertrages bedürfen der Schriftform.
2. Sollten in dieser Vereinbarung eine oder mehrere Bestimmungen unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Vertragsbestimmungen hierdurch nicht berührt. Die Vertragspartner werden die unwirksame oder undurchführbare Bestimmung durch eine Bestimmung ersetzen, die deren Sinn und Zweck am nächsten kommt. Gleiches gilt für den Fall einer ungewollten Regelungslücke.

Ort, Datum Ort, Datum

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

Unterschrift Verantwortlicher Unterschrift Auftragsverarbeiter

**Anhang 1: Angaben zum Auftragsverarbeiter**

**Datenschutzbeauftragter**

[x]  Der Auftragsverarbeiter hat einen Datenschutzbeauftragten bestellt. Dessen Kontaktdaten sind:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  Der Auftragsverarbeiter hat keinen Datenschutzbeauftragten bestellt. Dies ist nach den einschlägigen Regelungen des Datenschutzrechts aus folgenden Gründen nicht erforderlich:

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

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

**Vertreter des Auftragsverarbeiters**

[ ]  Der Auftragsverarbeiter ist nicht in der Union niedergelassen und benennt daher gemäß Art. 27 DSGVO folgenden Vertreter:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Organisation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Verlagerung der Datenverarbeitung in einen Staat außerhalb der Europäischen Union (Drittland)**

Die Auftragsverarbeitung in einem Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

[ ]  Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

[ ]  Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet (ggf. zusätzlich zu einem Mitgliedsstaat der Europäischen Union) in dem im Folgenden genannten Drittland statt. (Bei mehreren Drittländern oder Unterschiede für verschiedene Verarbeitungen ggf. Tabelle kopieren und ausfüllen.):

|  |  |
| --- | --- |
| Drittland |  |
| Betroffene Verarbeitung  |  |
| [ ]  Der Auftragsverarbeiter selbst erbringt die vereinbarte Datenverarbeitung (teilweise) im genannten Drittland |
| [ ]  Ein weiterer Auftragsverarbeiter (eine Firma) erbringt die vereinbarte Datenverarbeitung (teilweise) im genannten Drittland |
| Firma (Name, Anschrift) |  |
| Das Datenschutzniveau im Drittland | [ ]  ist festgestellt durch Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO),[ ]  wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m 47 DSGVO),[ ]  wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt c und d DSGVO),[ ]  wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 e i.V.m. 40 DSGVO),[ ]  wird hergestellt durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. F i.V.m. 42 DSGVO),[ ]  wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs. 2 lit a, Abs. 3 litt. a und b DSGVO):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| Drittland |  |
| Betroffene Verarbeitung  |  |
| [ ]  Der Auftragsverarbeiter selbst erbringt die vereinbarte Datenverarbeitung (teilweise) im genannten Drittland |
| [ ]  Ein weiterer Auftragsverarbeiter (eine Firma) erbringt die vereinbarte Datenverarbeitung (teilweise) im genannten Drittland |
| Firma (Name, Anschrift) |  |
| Das Datenschutzniveau im Drittland | [ ]  ist festgestellt durch Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO),[ ]  wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m 47 DSGVO),[ ]  wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt c und d DSGVO),[ ]  wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 e i.V.m. 40 DSGVO),[ ]  wird hergestellt durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. F i.V.m. 42 DSGVO),[ ]  wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs. 2 lit a, Abs. 3 litt. a und b DSGVO):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Versicherung**

[ ]  Der Auftragsverarbeiter verfügt über eine in Rahmen und Umfang marktübliche Haftpflichtversicherung oder eine vergleichbare Versicherung aus einem Mitgliedsstaat der EU und weist dies dem Verantwortlichen nach. Der Auftragsverarbeiter wird diesen Versicherungsschutz während der gesamten Vertragslaufzeit und bis zur Verjährung von Ansprüchen aufrechterhalten.

**Anhang 2: Details der Datenverarbeitung**

**Gegenstand des Auftrags**

Der Gegenstand des Auftrags ist …

*(Definition des Auftrags in Schlagworten, z. B. "Wartung des Schließsystems XY" oder genaue Bezeichnung eines zugrundeliegenden Vertrags, z. B. einer Leistungsvereinbarung, einer SLA etc. Ggf. Ergänzungen, z. B. "Eine Verarbeitung im Auftrag findet ausschließlich im Wege der Fernwartung oder vor Ort mit Betriebsmitteln des Verantwortlichen statt.")*

**Art und Zweck der Datenverarbeitung**

Die Art der Datenverarbeitung umfasst …

Zweck der Datenverarbeitung ist …

*(Beschreibung von Art (zu erbringenden Tätigkeiten) und Zweck der Datenverarbeitung durch den Auftragsverarbeiter oder Verweis auf ein Dokument in dem Art und Zweck konkret beschrieben werden, dann genaue Bezeichnung des Dokuments z. B. "Leistungsvereinbarung zu … vom ...")*

**Art der verwendeten Daten**

Gegenstand der Datenverarbeitung sind folgende Datenarten …

*(Beschreibung der Datenarten, z. B. Personenstammdaten, Arbeitsverträge, Arbeitszeiten, Videoaufzeichnungen, Kommunikationsdaten, Belegte Kurse, Prüfungsleistungen, oder Verweis auf ein Dokument in dem die Datenarten konkret beschrieben werden (s. o.)*

**Kategorien betroffener Personen**

Es werden im Rahmen des Auftrags personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet:

[ ]  Studierende

[ ]  Studienbewerber

[ ]  Beschäftigte

[ ]  Geschäftspartner

[ ]  Probanden

[ ]  …

*(Angabe der Kategorien betroffener Personen oder Verweis auf ein Dokument in dem die Datenarten konkret beschrieben werden (s. o.)*

**Anhang 3: Benennung von Ansprechpartnern gem. § 4**

Weisungsberechtige Personen im Hinblick auf die Datenverarbeitung nach dieser Auftragsverarbeitungsvereinbarung auf Seiten des Verantwortlichen sind:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Weisungsempfänger auf Seiten des Auftragsverarbeiters sind:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch Nachfolger bzw. Vertreter mitsamt Kontaktdaten mitzuteilen. Die Weisungen sind für die Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

**Anhang 4: Unterauftragsverhältnisse**

[ ]  Es findet keine Verarbeitung durch den Einsatz von weiteren Auftragsverarbeitern (Unterauftragnehmern) durch den Auftragsverarbeiter statt.

[ ]  Der Verantwortliche stimmt dem Einsatz der im Folgenden genannten weiteren Auftragsverarbeitern zu.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Anschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefon: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  Darüber hinaus ist der Einsatz von weiteren Auftragsverarbeitern durch den Auftragsverarbeiter nur mit vorheriger schriftlicher Zustimmung des Verantwortlichen im Einzelfall zulässig.

oder

[ ]  Darüber hinaus wird hiermit der Einsatz von weiteren Auftragsverarbeitern, die eine Niederlassung in einem Mitgliedsstaat der Europäischen Union haben oder für die ein Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO) einschlägig ist, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO genehmigt. Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtige Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter mindestens vier Wochen bevor die Änderung wirksam werden soll. Der Verantwortliche hat das Recht, gegen derartige Änderungen innerhalb von drei Wochen nach Zugang der Information Einspruch zu erheben. Der Einspruch steht einer Beauftragung von weiteren Auftragsverarbeitern entgegen.

Eine weitere Auslagerung durch einen weiteren Auftragsverarbeiter (Unterauftragnehmer) auf einen zusätzlichen weiteren Auftragsverarbeiter (Unter-Unterauftragnehmer)

[ ]  ist nicht gestattet;

[ ]  bedarf der ausdrücklichen Zustimmung des Verantwortlichen und der Auferlegung sämtlicher vertraglichen Regelungen in der Vertragskette an den zusätzlichen weiteren Auftragsverarbeiter.

**Anhang 5: Protokollierung der Fernwartung**

[ ]  Es findet eine Fernwartung statt, d. h. zu Wartungs- oder Reparaturzwecken erfolgen Zugriffe des Auftragsverarbeiters auf IT-Systeme des Verantwortlichen.

[ ]  Der Auftragsverarbeiter stellt dem Verantwortlichen eine Liste der Personen zur Verfügung die bei ihm potenziell die Möglichkeit eines Fernzugriffs auf das Netzwerk und die IT-Systeme des Verantwortlichen bekommen.

[ ]  Für jeden Fernzugriff werden von der ausführenden Person des Auftragsverarbeiters die folgenden Angaben in die Protokolldatei des Auftragsverarbeiters eingetragen:

Datum/Uhrzeit der Anmeldung

Dauer

Name

Zweck der Anmeldung (bspw. Einspielen des Patches <…>, Fehlersuche nach Incident <…>, …)

[ ]  Das Protokoll wird dem Verantwortlichen monatlich jeweils zum Monatsende zu Kontrollzwecken zur Verfügung gestellt.

**Anhang 6: Technisch-organisatorische Maßnahmen (TOMs)**

[ ]  Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Der Auftragsverarbeiter hat dazu folgendes Dokument erstellt:

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

Die in diesem Dokument festgelegten technischen und organisatorischen Maßnahmen sind Bestandteil dieser Vereinbarung.

oder

[ ]  Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen (TOM)

1. hinsichtlich der Sicherstellung der Vertraulichkeit,
2. hinsichtlich der Sicherstellung der Integrität,
3. hinsichtlich der Sicherstellung der Verfügbarkeit, Belastbarkeit sowie der Wiederherstellbarkeit nach einen physischen oder technischen Zwischenfall,
4. hinsichtlich der Pseudonymisierung und Verschlüsslung personenbezogener Daten,
5. hinsichtlich des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der TOM.

Die vom Auftragsverarbeiter getroffenen Maßnahmen sind entsprechend darzulegen, der Auftragsverarbeitung beizufügen. Sie sind Bestandteil dieser Vereinbarung.

Die im Folgenden aufgeführten Maßnahmen dienen ausschließlich als Beispiele.

1. **Vertraulichkeit (Artikel 32 Abs. 1 lit. b DSGVO)**

|  |  |  |
| --- | --- | --- |
|  | Anforderung | Beispielhafte Maßnahmen |
| a) | **Zutrittskontrolle**Kein unbefugter Zutritt zu Datenverarbeitungsanlagen | z. B. durch* Schlüssel, elektronische Schließung
* Protokollierung des Zutritts
* Verwaltung und Dokumentation von Zutrittsberechtigungen über den gesamten Lebenszyklus
* Werkschutz bzw. Pförtner
* Alarmanlage
* Videoüberwachung etc.
 |
| b) | **Zugangskontrolle**Keine unbefugte Systembenutzung | z. B. durch* (sichere) Kennwörter
* starke Authentisierung durch Zwei-Faktor-Authentifizierung
* automatische zeitabhängige Sperrmechanismen
 |
| c) | **Zugriffskontrolle** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems | z. B. durch* Berechtigungskonzept
* bedarfsgerechte (kleinstmögliche) Zugriffsrechte
* Protokollierung von Zugriffen
* regelmäßige Prüfung erteilter Berechtigungen (Audit) etc.
 |
| d) | **Trennungskontrolle**Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden | z. B. durch* getrennte Datenbanken
* Mandantenfähigkeit
* Sandboxing etc.
 |

1. **Integrität (Artikel 32 Abs. 1 lit. b DSGVO)**

|  |  |  |
| --- | --- | --- |
|  | Anforderung | Beispielhafte Maßnahmen |
| e) | **Weitergabekontrolle**Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport. | z. B. durch* (Transport)Verschlüsselung
* Virtual Private Network (VPN)
* (kryptologische) Hashfunktion etc.
 |
| f) | **Eingabekontrolle**Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. | z. B. durch: * Protokollierung
* Dokumentenmanagement etc.
 |

1. **Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b DSGVO)**

|  |  |  |
| --- | --- | --- |
|  | Anforderung | Beispielhafte Maßnahmen |
| g) | **Verfügbarkeitskontrolle**Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust | z. B. durch* Backup-Strategie (online/offline; on-site/off-site)
* Unterbrechungsfreie Stromversorgung (USV)
* Überwachung/Monitoring-Systeme
* Virenschutz
* Firewall
 |
| h) | **Rasche Wiederherstellbarkeit**  | z. B. durch* Redundanz
* Meldewege und Notfallpläne etc.
 |

1. **Pseudonymisierung (Artikel 32 Abs. 1 lit. a DSGVO; Artikel 25 Abs. 1 DSGVO)**

|  |  |  |
| --- | --- | --- |
|  | Anforderung | Beispielhafte Maßnahmen |
| e) | Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen (Artikel 4 Nr. 5 DSGVO). | z. B. durch* ersetzen von personenbezogenen Daten durch Zufallsdaten, Codes etc.
* Umsetzung von TOMs zum Schutz der Zuordnungsinformationen
 |

1. **Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

|  |  |  |
| --- | --- | --- |
|  | Anforderung | Beispielhafte Maßnahmen |
| e) | Unter Verschlüsselung versteht man Verfahren und Algorithmen, die Daten und Dateien (Text, Bild, Audio, Video, etc.) oder auch Netzwerkverbindungen mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht einfach lesbare, betrachtbare oder auslesbare Form umwandeln.  | z. B. durch* verschlüsselte Übertragung von Zugangsgeheimnissen (Credentials)
* Verschlüsselung von Datenträgern etc.
* Vgl. auch Weitergabekontrolle
 |

1. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d DSGVO; Artikel 25 Abs. 1 DSGVO)**

|  |  |  |
| --- | --- | --- |
|  | Anforderung | Beispielhafte Maßnahmen |
| e) | Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung | z. B. durch* Datenschutz-Management
* Incident-Response-Management
* Datenschutzfreundliche Voreinstellungen (Artikel 25 Abs. 2 DSGVO)
 |