Einzelkooperationsvereinbarung <Dienstbezeichnung>

Die <xxx>

– im Folgenden der „**Leistungserbringer**“ –

sowie

die <xxx>

– im Folgenden der „**Leistungsbezieher**“ –

– der Leistungserbringer und die Leistungsbezieher im Folgenden gemeinsam die „**Kooperationspartner**“ –

schließen folgende

Einzelkooperationsvereinbarung zur Nachnutzung des OZG-Online-Dienstes <Dienstbezeichnung>

Muster

Präambel

Die Kooperationspartner streben im Rahmen dieser Einzelkooperationsvereinbarung die zukunftsweisende und effiziente Umsetzung des vom IT-Planungsrat definierten Prinzips „Einer für Alle“ (EfA) für den OZG-Online-Dienst <Dienstbezeichnung> an. Diese Einzelkooperationsvereinbarung wird auf der Grundlage und im Rahmen der von Dataport AöR und d-NRW AöR geschlossenen „Vereinbarung über eine Zusammenarbeit zur Sicherstellung von digitalen und medienbruchfreien Verwaltungsleistungen von Bund, Ländern und Kommunen gegenüber Bürger*innen und Unternehmen“ (im Folgenden: „**IÖV**“) getroffen, der die FITKO und weitere Kommunalvertreter / öffentliche IT-Dienstleister der Länder beitreten können oder bereits beigetreten sind. Die IÖV ist am 20.10.2021 zwischen den ursprünglichen Kooperationspartnern in Kraft getreten und erstreckt ihre Wirksamkeit mit Beitritt auch auf weitere Kooperationspartner. Die Vereinbarungspartner nehmen zur Begründung der Einzelkooperationsvereinbarung Bezug auf die Präambel und die Anlage 1 der IÖV.

Es gelten sinngemäß die Allgemeine Vertragsbedingungen für den SaaS-Einstellungsvertrag (SaaS-Einstellungs-AGB) der FITKO in der zum Zeitpunkt des Abschlusses dieser Einzelvereinbarung gültigen Fassung. Die AGBs sind unter https://www.fitko.de/fit-store beziehbar. Zu den sinngemäßen Auslegungen gehören insbesondere die folgenden Aspekte:

1. Der Abschuss eines Einstellungsvertrages sowie Nachnutzungsvertrages ist nicht vorgesehen. Die notwendigen Regelungen zwischen Leistungserbringer und Leistungsbezieher werden in dieser Einzelvereinbarung geregelt.
2. Die Vereinbarungen werden demnach direkt zwischen Leistungserbringer und Leistungsbezieher geschlossen. Die Rolle des UL (Umsetzendes Land) gem. SaaS-Einstellungs-AGB wird durch den Leistungserbringer wahrgenommen. Die Rollen des AL (Anschließendes Land) sowie die Rolle der FITKO gem. SaaS-Einstellungs-AGB durch den Leistungsbezieher.
3. Die notwendigen individuellen Festlegungen des Einstellungsvertrages (gem. SaaS-Einstellungs-AGB) werden in Anlage 1 dieser Einzelvereinbarung festgeschrieben.
4. Die notwendigen individuellen Festlegungen der Leistungsbeschreibung (gem. SaaS-Einstellungs-AGB) werden in Anlage 2 dieser Einzelvereinbarung festgeschrieben.

§ 1
Gegenstand, Ziel und Zweck der Einzelkooperationsvereinbarung

I. Die Einzelkooperationsvereinbarung betrifft die Zusammenarbeit der Kooperationspartner, die der IÖV beigetreten sind, im Handlungsfeld 1 gemäß § 1 Absatz 1 Nr. 1 IÖV und die Umsetzung von OZG-Verwaltungsleistungen gemäß § 3 Absatz 1 IÖV.

II. Gegenstand der Einzelkooperationsvereinbarung sind mindestens der technische Betrieb und die damit verbundene fachliche Betreuung der OZG-Verwaltungsleistung (vgl. § 3 Abs. 1 IÖV)

„<OZG-Leistung> OZG-ID:<ID>“

(im Folgenden: „**OZG-Verwaltungsleistung**“) für die Nachnutzung dieser OZG-Verwaltungsleistung nach dem EfA-Prinzip nach § 2 Abs. 8 IÖV. Als weitere Gegenstände dieser Einzelkooperationsvereinbarung können darüber hinaus auch Wartung, Pflege und Weiterentwicklung geregelt werden. Hierzu bedarf es einer Konkretisierung in Anlage 1 (Konkretisierung der Betriebsvereinbarung sowie ggf. weiterer Leistungen und Abweichungen zu den SaaS-Einstellungs-AGB) und 2 (Leistungsbeschreibung) zu dieser Einzelkooperationsvereinbarung.

III. Die OZG-Verwaltungsleistung ist Teil des OZG-IP-Umsetzungskatalogs in der jeweils zum Abschluss dieser Einzelkooperationsvereinbarung geltenden Fassung mit den Merkmalen

Muster

EfA-fähig = Ja, EfA-Umsetzung = Ja, K-Paket finanzierbar = Ja, K-Paket finanziert = Ja und Priorität = 1.

IV. Ziel der Einzelkooperationsvereinbarung ist es, einen Beitrag dazu zu leisten, dass die teilweise noch fragmentierte IT-Landschaft im öffentlichen Interesse zu einem leistungsfähigen, interoperablen Plattformsystem ausgebaut wird, über das die Kooperationspartner ihre Verpflichtungen und Aufgaben nach dem OZG möglichst zügig und möglichst vollständig erfüllen bzw. wahrnehmen. Zweck der Einzelkooperationsvereinbarung ist es, das Zusammenwirken der Kooperationspartner bei der Umsetzung der in den Absätzen 1 und 2 genannten OZG-Verwaltungsleistung zur Erreichung der Ziele nach Satz 1 im Sinne der Grundsätze nach § 2 zu regeln.

§ 2
Grundsätze der Zusammenarbeit

Für die Zusammenarbeit der Kooperationspartner nach dieser Einzelkooperationsvereinbarung gelten die Grundsätze nach § 2 sowie nach § 4 Abs. 1 bis 3 IÖV.

§ 3
Pflichten des Leistungserbringers in Bezug auf die OZG-Online-Dienst

I. Der Leistungserbringer stellt dem Leistungsbezieher den OZG-Online-Dienst für den Nachnutzungszeitraum zur Nachnutzung bereit. Einzelheiten zum Betrieb des OZG-Dienstes sind in Anlage 1 (Konkretisierung der Betriebsvereinbarung sowie ggf. weiterer Leistungen und Abweichungen zu den SaaS-Einstellungs-AGB) aufgeführt.

II. Die fachliche und technische Beschreibung des OZG-Online-Dienstes erfolgt in Anlage 2 (Leistungsbeschreibung).

III. Die Weiterentwicklung des OZG-Online-Dienstes erfolgt gem. Ziff. 3.5 der SaaS-Einstellungs-AGB

§ 4
Nachnutzung

I. Mit Abschluss dieser Einzelkooperationsvereinbarung sind der Leistungsbezieher und die über ihn angeschlossenen Kommunen zur Nachnutzung des Online-Dienstes für den Nachnutzungszeitraum berechtigt. Abweichend von Ziff. 3.4.1 der SaaS-Einstellungs-AGB wird für den Nachnutzungszeitraum, also befristet, ein einfaches, nicht ausschließliches Nutzungsrecht an dem Dienst eingeräumt. Der Leistungsbezieher ist berechtigt, dieses einfache Nutzungsrecht für den Nachnutzungszeitraum an die ihm angeschlossenen Kommunen unterzulizenzieren. Eine weitere Berechtigung zur Unterlizenzierung oder Übertragung besteht nicht, weder für den Leistungsbezieher noch für die angeschlossenen Kommunen. Der Leistungsbezieher kann erklären, dass er eine Nachnutzung nur für bestimmte Kommunen oder öffentliche Einrichtungen in Anspruch nimmt; in jedem Fall müssen die nachnutzenden Kommunen und Einrichtungen im Einzelnen benannt werden. Dies erfolgt sinngemäß gem. der Vorgaben der Ziff. 2.2 der SaaS-Einstellungs-AGB. Nur für diesen Fall besteht das vorgenannte befristete Nutzungsrecht auch für die Kommune. Eine körperliche Überlassung des Online-Dienstes erfolgt nicht.

II. Abweichend von Ziff. 10.1 der SaaS-Einstellungs-AGB verpflichtet sich der Leistungsbezieher zum Leistungsbezug der OZG-Verwaltungsleistung ab dem <Datum> für einen Zeitraum von mindestens <xx> Monaten (Nachnutzungszeitraum). Der erste Nachnutzungs-

Muster

zeitraum endet abweichend am 31.12.2022. Im Hinblick auf die zum 31.12.2022 auslaufende Förderung durch das Konjunkturpaket und die notwendige Neuaufstellung der Finanzierung, verabreden sich die Kooperationspartner schon jetzt, rechtzeitig hierüber unter Einbeziehung des umsetzenden Landes zu verhandeln. Auf die Kündigungsregelungen in § 8 wird hingewiesen. Für den Fall der Kündigung endet das Nutzungsrecht für den Leistungsbezieher und die Kommunen mit dem Wirksamwerden der Kündigung.

III. Der Leistungsbezieher wirkt im Rahmen gesonderter Nutzungsvereinbarungen darauf hin, dass die „Anforderungen an EfA-mitnutzende Länder“ (Nachnutzende Länder/NL-Kriterien) gemäß den „Mindestanforderungen an ‚Einer für Alle‘-Services“ in der jeweils gültigen Fassung durch die nachnutzenden Kommunen erfüllt werden. Bei Nicht-Erfüllung der NL-Kriterien kann eine Nachnutzung nicht sichergestellt werden. Es besteht insoweit eine Mitwirkungspflicht.

§ 5
Finanzierung

I. Abweichend von Ziff. 3.6 der SaaS-Einstellungs-AGB sind die Kosten des Leistungserbringers bis zum 31.12.2022 durch Finanzmittel aus dem Konjunkturprogramm des Bundes für die Umsetzung des OZG nach dem EfA-Prinzip gedeckt. Für den Zeitraum bis zum 31.12.2022 erfolgt daher keine Kostenerstattung durch den Leistungsbezieher.

II. Ab dem 01.01.2023 erfolgt die Kostenerstattung durch <z.B. pauschal Land, individuell Kommune>, ggf. ebenfalls unter Hinweis auf eine von Ziff. 3.6 der SaaS-Einstellungs-AGB abweichende Regelung. Die Kooperationspartner werden sich hierzu rechtzeitig austauschen und dabei auch das umsetzende Land einbinden.

§ 6
Auftragsverarbeitung

I. Ergänzend zu Ziff. 9 der SaaS-Einstellungs-AGB gilt: Der Leistungserbringer ist gegenüber dem Leistungsbezieher Auftragsverarbeiter im Sinne des Art. 4 Ziff. 8 DSGVO. Es ist dafür ein Auftragsverarbeitungsvertrag gemäß den Vorgaben der DSGVO zu schließen. Die zwischen dem Leistungserbringer und dem Leistungsbezieher insoweit mit Abschluss dieser Einzelkooperationsvereinbarung geltenden Regelungen für die Auftragsverarbeitung sind als Anlage 3 beigefügt.

II. Der Leistungsbezieher ist gegenüber den nachnutzenden Kommunen / Stellen in <Bundesland> Auftragsverarbeiter im Sinne des Art. 4 Ziff. 8 DSG-VO. Er wird insoweit erforderliche Auftragsverarbeitungsvereinbarungen mit den nachnutzenden Kommunen und ggf. weiteren Intermediären selbst schließen. Dieses ist nicht die Aufgabe des Leistungserbringers.

§ 7
Haftung

Eine von den SaaS-Einstellung-AGB abweichende Haftung wird für den Fall vereinbart, dass der Leistungserbringer bereits anderslautende Haftungsregelungen für diesen Dienst geschlossen hat.

Für diesen Fall sind vorhandene Verträge des Leistungserbringers mit seinem Auftraggeber einzubeziehen. Die Haftung des Leistungserbringers gegenüber dem Leistungsbezieher bzw. gegenüber dem von dem Leistungsbezieher angeschlossenen Kommunen geht

in jedem Fall nicht weiter als die Haftung des Leistungserbringers aus dem vorhandenen Vertrag.

Die Abweichungen sind in Anlage 1 konkret zu benennen.

§ 8
Laufzeit, Kündigung

I. Diese Einzelkooperationsvereinbarung wird auf unbestimmte Zeit geschlossen.

II. Die Kooperationspartnerpartner können die Einzelkooperationsvereinbarung unter Einhaltung einer Frist von sechs Monaten zum Ende eines Nachnutzungszeitraums, frühestens jedoch zum 31.12.2022 kündigen.

III. Das Recht der Kooperationspartner zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§ 9
Allgemeine Bestimmungen und Vertraulichkeit

I. Ergänzend zu Ziff. 11.1 der SaaS-Einstellungs-AGB sind Nebenabreden, Änderungen und Ergänzungen dieser Einzelkooperationsvereinbarung nur im Einvernehmen zwischen den Vereinbarungspartnern möglich und bedürfen der Schriftform.

II. Sollten einzelne Bestimmungen dieser Einzelkooperationsvereinbarung ganz oder teilweise unwirksam oder unanwendbar sein oder werden, so wird die Gültigkeit der übrigen Bestimmungen hiervon nicht berührt. Die Kooperationspartner verpflichten sich, in einem solchen Fall an der Schaffung von Bestimmungen mitzuwirken, durch die ein der nichtigen oder unwirksamen Bestimmung rechtlich oder wirtschaftlich möglichst nahekommendes Ergebnis rechtswirksam erzielt wird. Dasselbe gilt für etwaige Regelungslücken.

III. Sind Bestimmungen dieser Einzelkooperationsvereinbarung auslegungs- oder ergänzungsbedürftig, so hat die Auslegung oder Ergänzung in der Weise zu erfolgen, dass sie dem Geist, Inhalt und Zweck dieser Einzelkooperationsvereinbarung bestmöglich gerecht wird. Dabei soll diejenige Regelung gelten, die die Kooperationspartner bei Abschluss dieser Einzelkooperationsvereinbarung getroffen hätten, wenn sie die Auslegungs- oder Ergänzungsbedürftigkeit erkannt hätten.

IV. Treten Widersprüche zwischen dieser Einzelkooperationsvereinbarung und der IÖV auf, hat die Regelung aus der Einzelkooperationsvereinbarung Vorrang.

Anlagen als Vertragsbestandteile:

- Anlage 1: Konkretisierung der Betriebsvereinbarung sowie ggf. weiterer Leistungen und Abweichungen zu den SaaS-Einstellungs-AGB
- Anlage 2: Leistungsbeschreibung
- Anlage 3: Vereinbarung zur Auftragsverarbeitung mit konkretisierenden Anhängen

Leistungserbringer, <xxx> Leistungsbezieher, <xxx>

Muster

(Ort, Datum)	(Ort, Datum)
(Unterschrift)	(Unterschrift)

Muster

Anlage 1 zur Einzelkooperationsvereinbarung <Dienstbezeichnung>:

Konkretisierung der Betriebsvereinbarung sowie ggf. weiterer Leistungen und Abweichungen zu den SaaS-Einstellungs-AGB (Muster; die Anlage 1 kann auch individuell erstellt werden, solange sie die aufgeführten Inhalte umfasst)

Konkretisierung des Inhalts der Leistung (Betrieb, Wartung, Pflege, Weiterentwicklung):

<xxx>

Abweichend von den SaaS-Einstellungs-AGB werden folgende Inhalte individuell vereinbart:

<xxx>

Weitergehende Informationen:

1.1 Servicestelle des IT-Dienstleisters

Servicestelle des IT-Dienstleisters (Name/Stelle, Adresse, Abteilung, Telefon, Fax, E-Mail):

1.2 Störungsmeldung

Die Meldung einer Störung des Online-Dienstes erfolgt wie folgt:

2 Ansprechpersonen/Ansprechstelle

Ansprechpersonen/Ansprechstelle von Leistungsbezieher (Name/Stelle, Adresse, Abteilung, Telefon, Fax, E-Mail):

Ansprechpersonen/Ansprechstelle von Leistungserbringer (Name/Stelle, Adresse, Abteilung, Telefon, Fax, E-Mail):

3 IT-Dienstleister

Der Leistungserbringer ist berechtigt, für die von ihm zu erbringenden Leistungen folgende IT-Dienstleister einzusetzen**:**

4 Schlichtung

Die Vertragsparteien vereinbaren gemäß Ziffer 11.2 SaaS-Einstellungs-AGB, folgende Schlichtungsstelle anzurufen:

5 Sonstige Vereinbarungen

Muster

Anlage 2 zur Einzelkooperationsvereinbarung <Dienstbezeichnung>:

Leistungsbeschreibung (Muster; die Anlage 2 kann auch individuell erstellt werden, solange sie die aufgeführten Inhalte umfasst)

1. Inhalt des Online-Dienstes / der Leistung

1.1 Welche Verwaltungsleitung(en) werden mit dem Online-Dienst abgebildet bzw. erfasst?

1.2 Falls gelistet gem. „Leistungskatalog der öffentlichen Verwaltung“ (Leika) bitte entsprechender Bezeichnung angeben:

2 FIM-Leistungsbeschreibung der Verwaltungsleistungen

Bitte fügen Sie hier einen Link zur Leistungsbeschreibung ein (z.B. vom FIM-Portal)

3 Funktionsweise und -umfang des Online-Dienstes

3.1 Beschreibung der Funktionsweise

(Beschreiben Sie die Funktionsweise und den Umfang Ihres Online-Dienstes. Orientieren Sie Ihre Beschreibung an der (Ablauf-) Strecke von der Anmeldung über ein Konto X auf Vertrauensniveau Y, Verarbeitung/Zwischenspeicherung von Daten, Verschlüsselung, Validierung von Eingaben bis zur Übergabe der Daten an Behörde.)

3.2 Architektur-, Datenflussdiagramme, Übersichtsdarstellungen o. ä.

4 Systemumgebung

Technische Beschreibung des Online-Dienstes, insbesondere

- Vorgesehene Art der Datenübermittlung (Fachverfahrensanbindung, Postkorblösung, etc.) und genutzte Datenaustauschstandards:
- Anbindungsmöglichkeiten an den Online-Dienst für den Leistungsbezieher (Schnittstellen, verwendete Fachstandards)
- Erforderliche Basisdienste bei dem Leistungsbezieher:
- Sonstige technische Voraussetzungen, die für den Leistungsbezieher relevant sind (ggf. Verweis auf Mindestanforderungen an „EfA“-Serviceleistungen)

5 Leistungsabgrenzung

Teilen Sie mit was ggf. nicht enthalten ist:

6 Sonstige Vereinbarungen zur Leistungsbeschreibung

Zusätzlich zu den in Anlage 1 zur Einzelkooperationsvereinbarung geregelten Angaben werden folgende Vereinbarungen zur Leistungsbeschreibung festgelegt:

Muster

Anlage 3 zur Einzelkooperationsvereinbarung <Dienstbezeichnung>:

Vereinbarung zur Auftragsverarbeitung

Zwischen der

[Titel/Name]

- nachstehend „**Auftragnehmer/Leistungserbringer**“ genannt –

und

[Titel/Name]

- nachstehend „**Auftraggeber/Leistungsbezieher**“ genannt -

- beide nachstehend gemeinsam „**Vertragsparteien**“ genannt –

wird die folgende Vereinbarung zur Auftragsverarbeitung (nachstehend „Vertrag“) als Anlage 3 zur Einzelkooperationsvereinbarung <Dienstbezeichnung> geschlossen:

Präambel

Die Vertragsparteien bezwecken mit dem Vertrag ein Auftragsverarbeitungsverhältnis einzugehen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung („**DSGVO**“), des Bundesdatenschutzgesetzes („**BDSG**“) sowie der Datenschutzgesetze der jeweiligen Länder in der jeweils gültigen Fassung zu konkretisieren, schließen die Vertragsparteien den nachfolgenden Vertrag.

1 Definitionen

(1) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.

(2) Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit der Vertrag eine andere Form ausdrücklich vorsieht.

2 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer erhält Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend „**Auftraggeberdaten**“) und verarbeitet diese für den Auftraggeber in dessen Auftrag und nach dessen Weisungen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO. Der Gegenstand des Auftrages ergibt sich aus §1 der Einzelkooperationsvereinbarung sowie der Anlagen 1 und 2 zur Einzelkooperationsvereinbarung.

Muster

(2) Die Verarbeitung von Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in Anhang 1 zu diesem Vertrag spezifiziert. Die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers Änderungen der Festlegungen in **Anhang 1** dieses Vertrags zuzustimmen, soweit er keinen sachlichen Grund zur Verweigerung dieser Zustimmung hat. Die Änderungen sind schriftlich festzulegen.

(3) Die Dauer der Verarbeitung ergibt sich aus der Dauer der Einzelvereinbarung.

(4) Jede von den Festlegungen in **Anhang 1** des Vertrags abweichende oder darüberhinausgehende Verarbeitung von Auftraggeberdaten ist dem Auftragnehmer untersagt, insbesondere eine Verarbeitung der Auftraggeberdaten zu eigenen Zwecken. Das gilt auch für den Fall einer Verwendung anonymisierter Daten.

(5) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer findet ausschließlich in Mitgliedstaaten der Europäischen Union **("EU")** oder Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum **("EWR")** statt.

Eine Datenverarbeitung außerhalb der EU oder des EWR, auch im Wege der Gewährung des Zugriffs auf Auftraggeberdaten, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Datenverarbeitung in Ländern, die weder Mitgliedstaat der EU oder Vertragsstaat des EWR sind (nachfolgend „Drittländer" genannt) dürfen nur dann und soweit erfolgen, dass die Voraussetzungen der Art. 44 ff. DSGVO zur Zufriedenheit des Auftraggebers erfüllt sind.

3 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer darf die Auftraggeberdaten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftraggeber besitzt insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang, Zweck und Verfahren der Verarbeitung von Auftraggeberdaten. Die Weisungen des Auftraggebers sollen grundsätzlich in Schrift- oder Textform erfolgen. Bei Bedarf kann der Auftraggeber Weisungen auch mündlich oder telefonisch erteilen. Mündlich oder telefonisch erteilte Weisungen bedürfen jedoch einer unverzüglichen Bestätigung des Auftraggebers in Schrift- oder Textform. Der Auftragnehmer ist verpflichtet, sämtliche Weisungen des Auftraggebers zu dokumentieren.

(3) Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.

(4) Der Auftragnehmer gewährleistet, dass er die Auftraggeberdaten im Einklang mit den Bestimmungen dieses Vertrags und den Weisungen des Auftraggebers verarbeitet. Der Auftragnehmer bestätigt, dass ihm und seinen Mitarbeitern, die mit Auftraggeberdaten umgehen, die Vorschriften der DSGVO und die sonstigen einschlägigen Datenschutzvorschriften bekannt sind. Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber mit mindestens 14-tägiger Frist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.

Muster

4 Anforderungen an Personal und Systeme

(1) Der Auftragnehmer hat alle Personen, die Auftraggeberdaten verarbeiten, bezüglich der Verarbeitung von Auftraggeberdaten in Schriftform zur Vertraulichkeit während und nach Beendigung ihres Beschäftigungsverhältnisses zu verpflichten, soweit diese nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(3) Die Einhaltung dieser Verpflichtung ist dem Auftraggeber auf Anfordern nachzuweisen.

(4) Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeberdaten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der EU oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

(5) Der Auftragnehmer gewährleistet, dass er nur solche Systeme für die Verarbeitung von Auftraggeberdaten einsetzt, die dafür ausgelegt sind, den Datenschutz durch eine der Verarbeitungssituation angemessene technische Systemgestaltung zu unterstützen.

5 Weitere Pflichten des Auftragnehmers

(1) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutz-Folgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(2) Soweit nach Art. 37 Abs. 1 DSGVO oder anderweitig gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenkonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit. Wurde kein Beauftragter bestellt, teilt der Auftragnehmer dem Auftraggeber einen Ansprechpartner für anfallende Datenschutzfragen mit.

6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer gewährleistet, alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen und während der Dauer der Verarbeitung von Auftraggeberdaten aufrecht zu erhalten, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeberdaten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeberdaten zu gewährleisten. Die in **Anhang 2** des Vertrags beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die diesem Vertrag oder seiner **Anhang 2** nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung des Sicherheitsniveaus erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Vertragsparteien zu vereinbaren und zu dokumentieren. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(3) Die Verarbeitung von Daten in Privatwohnungen (z.B. bei Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird, die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

(4) Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(5) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

7 Unterauftragsverhältnisse

(1) Die gegenwärtig vom Auftragnehmer eingesetzten Subunternehmer sind in **Anhang 3** des Vertrags genannt, mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und der Auftraggeber erteilt mit Abschluss dieses Vertrages seine Zustimmung zum Einsatz dieser Subunternehmer.

(2) Verträge mit Subunternehmern sind in schriftlicher oder elektronischer Form zu vereinbaren und müssen dem Subunternehmer mindestens mit diesem Vertrag vergleichbare Datenschutzpflichten auferlegen, insbesondere die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen umfassen. Der Auftragnehmer wird sicherstellen, dass der Auftraggeber auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer erhalten kann.

(3) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung weiterer oder Ersetzung bestehender Subunternehmer informieren. Die Hinzuziehung oder Ersetzung bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers, welche dieser nicht unbillig verweigern wird. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt und die Anforderungen an Subunternehmerverträge gemäß vorstehendem Absatz 2 erfüllt sind.

(4) Im Falle der Zustimmung wird der Auftragnehmer die Liste der Subunternehmer in **Anhang 3** entsprechend aktualisieren und dem Auftraggeber unverzüglich zur Verfügung stellen.

Muster

(5) Der Auftragnehmer wählt Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO sorgfältig aus. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen. Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Subunternehmer geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeberdaten gemäß diesem Vertrag erfolgt.

(6) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich in einem Mitgliedstaat der EU oder eines Vertragsstaates des EWR erbringen, ist nur bei Beachtung der in Ziffer 2 Abs.5 dieses Vertrages genannten Bedingungen möglich.

(7) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber wie für eigenes Verschulden.

8 Rechte der Betroffenen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte von Betroffenen ist der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

(3) Der Auftragnehmer wird den Auftraggeber insbesondere unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeberdaten unmittelbar an den Auftragnehmer wenden sollte und dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeberdaten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen,

einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen (etwa nach Art. 33 oder 34 DSGVO) auf erstes Anfordern im Rahmen des Zumutbaren zu unterstützen. Der Auftragnehmer wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeberdaten zu minimieren und zu beseitigen, die Auftraggeberdaten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.

(3) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer - soweit erforderlich - Zutritt und Einblick zu ermöglichen. Der Auftragnehmer sichert zu, dass er bei den Kontrollen – soweit erforderlich – unterstützend mitwirkt. Er ist insbesondere verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Ziffer 10 Abs. 3 dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(3) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit - z.B. nach BSI-Grundschutz - („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

(4) Der Auftragnehmer unterwirft sich der Kontrolle des behördlichen Datenschutzbeauftragten der d-NRW Anstalt öffentlichen Rechts. Er gestattet diesem sowie den für ihn tätigen Personen während der üblichen Geschäftszeiten den Zutritt zu seinen Geschäftsräumen und gewährt Zugang zu den Datenverarbeitungsanlagen und Unterlagen. Der Auftragnehmer ist verpflichtet, Anfragen des Datenschutzbeauftragten unverzüglich und vollständig zu beantworten.

(5) Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die ver-

tragsgegenständliche Verarbeitung von Auftraggeberdaten Gegenstand des Aufsichtsverfahrens ist. Der Auftragnehmer wird insbesondere auf Verlangen des Auftraggebers ihm selbst oder der Aufsichtsbehörde unmittelbar alle Informationen im Zusammenhang mit diesem Vertrag geben und entsprechende Auskünfte erteilen und der Aufsichtsbehörde die Möglichkeit einräumen, Prüfungen in demselben Umfang durchzuführen, wie sie die Aufsichtsbehörde beim Auftraggeber durchführen darf. Der Auftragnehmer verpflichtet sich, der zuständigen Aufsichtsbehörde auch in diesem Rahmen alle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu gewähren. Falls die Aufsichtsbehörde beim Auftragnehmer Kontrollhandlungen, Ermittlungen oder Maßnahmen durchführt, die Auftraggeberdaten betreffen, hat der Auftragnehmer den Auftraggeber darüber so früh wie möglich und in der Regel unverzüglich nach Erhalt der Ankündigung der Aufsichtsmaßnahme durch die Behörde zu informieren.

11 Pflichten nach Beendigung des Vertrags

(1) Bei Beendigung dieses Vertrages oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder unwiderruflich zu vernichten oder an den Auftraggeber zu übergeben, sofern nicht eine gesetzliche Pflicht zur Speicherung der personenbezogenen Daten besteht. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Es ist eine dem Risiko des Schutzbedarfes der Daten angemessene Vernichtung durchzuführen.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Gesetzliche Aufbewahrungspflichten des Auftragnehmers bleiben von den vorstehenden Regelungen unberührt. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter diesem Vertrag verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Beschäftigten bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subunternehmer im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13 Sonstiges

(1) Im Falle von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere der Einzelvereinbarung, gehen die Regelungen dieses Vertrags vor.

Muster

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrages im Übrigen nicht. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

(6) Dieser Vertrag unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist <xx>.

Anhang 1 zur Anlage 3 – Datenkategorien, Zwecke, Betroffene

Der Auftragnehmer verarbeitet die folgenden personenbezogenen Daten:

I. Zwecke

xx

II. Betroffene

- *xxx*

III. Datenkategorien

- *xxx*

Anhang 2 zur Anlage 3 – Technische und organisatorische Maßnahmen (TOM)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Für die Bestimmung geeigneter TOM ist zunächst der Schutzbedarf der zu verarbeitenden personenbezogenen Daten festzulegen und hier zu dokumentieren.

Schutzbedarf der Daten gemäß Systematik der DSK: Klicken oder tippen Sie hier, um Text einzugeben.

Es müssen Regelungen zu folgenden Punkten getroffen werden:

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse [1, 2 oder 3].

Muster

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

>> Zutrittskontrolle

Folgende Maßnahmen sind umzusetzen, um den unbefugten Zutritt zu Datenverarbeitungsanlagen und Daten zu verhindern: [*z. B.*

- *Verwendung von Sicherheitsschlössern an Zugangstüren*
- *Festlegung einer Schlüsselregelung, durch die ein möglichst kleiner Personenkreis uneingeschränkten Zugang erhält*
- *bei Generalschlüsselanlage Quittierung der Ausgabe des Generalschlüssels*
- *wenn möglich, vom Publikumsverkehr räumlich abgegrenzte PC-Arbeitsplätze, Server und andere Speichermedien sowie Aufbewahrungsorte von Akten*]

>> Zugangskontrolle

Folgende Maßnahmen sind umzusetzen, um eine unbefugte (System-) Benutzung zu verhindern: [*z. B.*

- *Benutzerkennung mit sicheren Kennwörtern*
  - *unterschiedlichen Zeichenzusammensetzung, Mindestlänge 8 Zeichen, regelmäßiger Wechsel*
  - *Bildschirmsperre bei Pausen mit Passwort-Aktivierung*
  - *Zugangssperre bei mehr als 3 Anmeldeversuchen*
  - *Vermeidung der Verwendung von Gruppen-Passwörter*
- *Firewall inkl. Zugriffs- und Änderungsberechtigungskonzept*
- *Einsatz von Anti-Viren-Software*
- *Regelmäßige Aktualisierung von Sicherheitspaketen bei Programmen, die mit dem Internet verbunden sind*
- *Sicherung und Verschlüsselung von Datenträgern*
- *bei externer Systemadministration Schließung einer Vereinbarung zur Auftragsdatenverarbeitung*
- *sorgfältige Auswahl des Sicherheits- und Reinigungspersonals*]

>> Zugriffskontrolle

Folgende Maßnahmen sind umzusetzen, damit die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und damit personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können: [*z. B.*

- *Benutzerkennung mit sicheren Kennwörtern (siehe auch Zugangskontrolle)*
- *Datenträgerverwaltung inkl. Benennung eines Verantwortlichen*
- *bedarfsgerechte Zugriffsrechte (z.B. für Praktikanten und studentische Hilfskräfte)*
- *gesicherte Schnittstellen (insbesondere bei aktiven Netzkomponenten)*
- *Aufbewahrung von sensiblen Akten in verschließbaren Schränken und Einsatz von Aktenvernichtern*]

2. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

>> Verfügbarkeitskontrolle

Folgende Maßnahmen sind zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust umzusetzen: [*z. B.*

- *Brandschutzmaßnahmen*
  - *Feuerlöscher an/in den PC- Arbeitsräumen und Aktenaufbewahrungsräumen*
  - *Wenn möglich Brandschutztüren*
  - *Rauchverbot an/in den PC- Arbeitsräumen und Aktenaufbewahrungsräumen*

Muster

- *Backupkonzept, z.B. Festplattenspiegelung, Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort*
- *Einsatz von Anti-Viren-Software*
- *Schutz vor Diebstahl (siehe auch Zutritts- und Zugangskontrolle)*
- *Testen von Datenwiederherstellung*]

3. Verfahren zur regelmäßigen Überprüfung,

Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

>> Datenschutz-Management

Der Auftragnehmer ist für die Umsetzung der hier genannten technischen und organisatorischen Maßnahmen zuständig und plant, organisiert, steuert und kontrolliert systematisch die gesetzlichen und betrieblichen Anforderungen des Datenschutzes.

>> Incident-Response-Management

Die Verletzung des Schutzes personenbezogener Daten ist gegenüber dem Auftraggeber unverzüglich zu melden. Ferner sind Art. 33 und 34 DSGVO zu beachten.

>> Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Soweit es die Art der zur Verarbeitung vorgesehenen Daten zulässt, ist darauf zu achten, dass diese pseudonymisiert werden.

>> Auftragskontrolle

Folgende Maßnahmen dienen der Verhinderung einer Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers:

- Beachtung der Weisungsbefugnis
- Kontrollen vor Ort

Anhang 3 zur Anlage 3 – Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Kontaktperson	Anschrift	Leistung
1				
2				
3				

Muster

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
_____	_____
Name, Vorname, Funktion des/der Vertretungsberechtigten	Name, Vorname, Funktion des/der Vertretungsberechtigten

Muster