# Vertrag zur Auftragsverarbeitung personenbezogener Daten gemäß § 29 KDG

# Vereinbarung

zwischen   der   

  Einrichtung inkl. Anschrift     
- Verantwortlicher -  
nachstehend **Auftraggeber** genannt

und   der

  Einrichtung/Firma inkl. Anschrift      
- Auftragsverarbeiter -  
nachstehend **Auftragnehmer** genannt

**Hinweis**Die einzelnen Festlegungen nach § 29 Abs. 3 KDG sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.

###### **1. Gegenstand und Dauer des Auftrags**

**(1) Gegenstand**

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/      vom      , auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

  (Definition der Aufgaben)

**(2) Dauer**

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum      .

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von       zum       gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

###### **2. Konkretisierung des Auftragsinhalts**

**(1) Art und Zweck der vorgesehenen Verarbeitung von Daten**

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom      .

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen gem. § 29 Abs. 11 KDG erfüllt sind. Das angemessene Schutzniveau in Land hier einfügen

ist festgestellt durch einen Angemessenheitsbeschluss der Kommission Art. 45 Abs. 3 DS-GVO);

wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO)

wird hergestellt durch Standarddatenschutzklauseln (§ 29 Abs. 7 und 8 KDG);

wird hergestellt durch genehmigte Verhaltensregeln gemäß § 29. Abs. 6 KDG und Art. 40 DS-GVO);

wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (§ 29 Abs. 6 KDG und Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

wird hergestellt durch sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**(2) Art der Daten**

Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:

oder

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

Personenstammdaten

Kommunikationsdaten (z. B. Telefon, E-Mail)

Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

Kundenhistorie

Vertragsabrechnungs- und Zahlungsdaten

Planungs- und Steuerungsdaten

Gesundheitsdaten

Biometrische Daten

Bilddateien

Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

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

**(3) Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

oder

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kunden

Interessenten

Abonnenten

Beschäftigte

Lieferanten

Handelsvertreter

Ansprechpartner

Patienten

Klienten

Bewohner

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

###### **3. Technisch-organisatorische Maßnahmen**

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. § 26 KDG insbesondere in Verbindung mit § 7 KDG herzustellen. 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, 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 § 26 Abs. 1 lit. d zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

###### **4. Berichtigung, Einschränkung und Löschung von Daten**

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

**Info:** Der Auftraggeber kann vertraglich zur Übernahme der anfallenden Mehrkosten verpflichtet werden.

###### **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a)  Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß § 38 KDG ausübt.

Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b)  Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c)  Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß § 29 Abs. 4 lit. b KDG. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

**Info:** Eine gesetzliche Verpflichtung zur Verarbeitung kann z. B. bei Herausgabeverlangen von Ermittlungsbehörden bestehen.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß § 26 KDG [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

**Info:** Der Auftraggeber kann vertraglich zur Übernahme der anfallenden Mehrkosten verpflichtet werden. Der Auftragnehmer kann wegen fehlender Kostenübernahme durch den Auftraggeber jedoch kein Leistungsverweigerungsrecht gegenüber der Behörde geltend machen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

**Info:** Zum sog. PDCA-Zyklus („plan-do-check-act“) siehe GDD-Praxishilfe DS-GVO II „Verantwortlichkeiten und Zuständigkeiten nach der DS-GVO“, Punkt 2.1.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

k) Der Auftragnehmer verpflichtet sich die ihm ggf. zugänglich gemachten Privatgeheimnisse mit Sorgfalt zu behandeln und sie keinem Dritten zugänglich zu machen, da er sich ansonsten nach § 203 Abs. 4 StGB strafbar macht. Der Wortlaut des Strafgesetzbuches ist beigefügt.

*§ 203 Strafgesetzbuch*

*(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als*

1. *Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,*
2. *Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,*
3. *Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,*
4. *Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,*
5. *Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,*
6. *staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder*
7. *Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle*

*anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*

*(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.*

###### **6. Unterauftragsverhältnisse**

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a)  Eine Unterbeauftragung ist unzulässig.

b)  Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des § 29 KDG:

|  |  |  |
| --- | --- | --- |
| Firma Unterauftragnehmer | Anschrift/Land | Leistung |
|  |  |  |
|  |  |  |

c)  Die Auslagerung auf Unterauftragnehmer ist zulässig, soweit:

* der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

**Info:** Ggf. ist die Vereinbarung einer Meldefrist (bspw. 2 Wochen) sowie eine Festlegung einer Frist vor dem Zeitpunkt der Übergabe der Daten ratsam.

* der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
* eine vertragliche Vereinbarung nach Maßgabe des § 29 KDG zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

ist nicht gestattet;

bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

###### **7. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach § 29 KDG überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO ;

die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

###### **8. Mitteilung bei Verstößen des Auftragnehmers**

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der der gesetzlich festgelegten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

**Info:** Auf welche Weise der Auftragnehmer den Auftraggeber unterstützt, ist von der Art der Dienstleistung abhängig. Entsprechende Maßnahmen sollten vertraglich konkretisiert werden.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

###### **9. Weisungsbefugnis des Auftraggebers**

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

**Info:** Die Ziffer 9 wurde im neuen Muster erheblich verschlankt. Die allgemeinen Regeln zur Weisungsbefugnis finden sich bereits in Ziffer 5 lit. d (Qualitätssicherung) des Musters. Ziffer 9 ist Besonderheiten vorbehalten.

###### **10. Löschung von Daten und Rückgabe von Datenträgern**

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

# ANLAGE 1: Allgemeine technische und organisatorische Maßnahmen gem. § 26 KDG

1. **Vertraulichkeit**

**Zutrittskontrolle**

*Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.*

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Bitte kreuzen Sie Ihre Maßnahmen an:

Zutrittskontrollsystem

Ausweisleser, Magnetkarte, Chipkarte

Schlüssel/Schlüsselvergabe

Türsicherung (elektrische Türöffner usw.)

Werkschutz, Pförtner

Überwachungseinrichtung

Alarmanlage, Video-/Fernsehmonitor

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Zugangskontrolle**

*Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.*

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Bitte kreuzen Sie Ihre Maßnahmen an:

Kennwortverfahren (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)

Automatische Sperrung (z. B. Kennwort oder Pausenschaltung)

Einrichtung eines Benutzerstammsatzes pro User

Verschlüsselung von Datenträgern

Erstellen von Benutzerprofilen

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Zugriffskontrolle**

*Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.*

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Bitte kreuzen Sie Ihre Maßnahmen an:

Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)

Protokollierung von Zugriffen

Auswertungen

Kenntnisnahme

Veränderung

Löschung

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Trennungskontrolle**

*Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.*

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Bitte kreuzen Sie Ihre Maßnahmen an:

"Interne Mandantenfähigkeit"/Zweckbindung

Sandboxing

Funktionstrennung/Produktion/Test)

Physikalisch getrennte Speicherung

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pseudonymisierung**

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 technische und organisatorischen Maßnahmen unterliegen.

Bitte kreuzen Sie Ihre Maßnahmen an:

Nutzung von Identifikationsnummern (z. B. Personalnummer, Matrikelnummer, Mitgliedsnummer)

Verwendung von „Nicknames“

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2. Integrität**

**Weitergabekontrolle**

*Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ...*

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Bitte kreuzen Sie Ihre Maßnahmen an:

Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network)

Elektronische Signatur

Protokollierung

Transportsicherung

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Eingabekontrolle**

*Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.*

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Bitte kreuzen Sie Ihre Maßnahmen an:

Protokollierungs- und Protokollauswertungssysteme

Dokumentenmanagement

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.** **Verfügbarkeit und Belastbarkeit**

**Verfügbarkeitskontrolle**

*Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.*

Maßnahmen zur Datensicherung (physikalisch/logisch):

Bitte kreuzen Sie Ihre Maßnahmen an:

Backup-Verfahren

Spiegeln von Festplatten, z. B. RAID-Verfahren

Unterbrechungsfreie Stromversorgung (USV)

Getrennte Aufbewahrung

Virenschutz/Firewall

Notfallplan

Feuerlöschgeräte in Serverräumen

Klimaanlage in Serverräumen

Meldewege

Rasche Wiederherstellbarkeit

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4.** **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

**Datenschutz-Management**

**Datenschutzfreundliche Voreinstellungen § 27 KDG**

**Auftragskontrolle**

*Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.*

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Bitte kreuzen Sie Ihre Maßnahmen an:

Eindeutige Vertragsgestaltung

Formalisierte Auftragserteilung (Auftragsformular)

Kriterien zur Auswahl des Auftragnehmers

Kontrolle der Vertragsausführung

Vertragsstrafen bei Verstößen

Sonstige Maßnahmen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Keine Auftragsdatenverarbeitung im Sinne von § 29 KDG ohne entsprechende Weisung des Auftraggebers, z. B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

|  |  |
| --- | --- |
| Ort, Datum | Unterschrift Auftraggeber |

|  |  |
| --- | --- |
| Ort, Datum | Unterschrift Auftragnehmer |