Muster

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DS-GVO

zwischen

Kommunales Jobcenter Hamm AöR

Wilhelmstraße 189

59067 Hamm

als Verantwortliche/r - nachfolgend "**Auftraggeber**" genannt –

und

_____

_____

_____

als Auftragsverarbeiter/in - nachfolgend "**Auftragnehmer**" genannt –

- Auftraggeber und Auftragnehmer nachfolgend jeder auch "Partei" und gemeinsam "Parteien" -

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich _____
_____
_____ (kurze Beschreibung)
gemäß Vertrag vom _____ (im Folgenden: "**Hauptvertrag"**). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("**DS-GVO**"). Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird.

§ 1 Gegenstand/Umfang der Beauftragung

(1) Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "**Auftraggeberdaten**") erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DS-GVO verarbeitet.

(2) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich in der in **Anlage 1** spezifizierten Art sowie zu dem dort spezifizierten Zweck. Die Art der verarbeiteten Daten und der Kreis der von der Datenverarbeitung betroffenen Personen ist ebenfalls in **Anlage 1** zu diesem Vertrag dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Dem Auftragnehmer ist eine abweichende oder über die Festlegungen in der **Anlage 1** hinausgehende Verarbeitung von Auftraggeberdaten untersagt. Dies gilt auch für die Verwendung anonymisierter Daten.

(4) Die Verarbeitung der Auftraggeberdaten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verarbeitung in Drittländern ist zulässig, soweit ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht.

(5) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch

den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

§ 2 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers iSv Art. 28 DS-GVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "**Weisungsrecht**"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer schriftlich zu bestätigen. Der Auftragnehmer dokumentiert die Weisungen des Auftraggebers. Die weisungs- und empfangsberechtigten Personen ergeben sich aus **Anlage 2**. Bei einem Wechsel oder einer längerfristigen Verhinderung der in **Anlage 2** benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Der Auftragnehmer wird dem Auftraggeber einen Wechsel der Person des Empfangsberechtigten frühzeitig anzeigen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 3 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden "**Mitarbeiter**" genannt), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DS-GVO, insbesondere die in **Anlage 3** zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß **Anlage 3** nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in **Anlage 3** bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

§ 4 Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich,

spätestens aber innerhalb von 24 Stunden in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen gemäß § 4 Abs. 1 Satz 1 enthalten jeweils zumindest die in Art. 33 Absatz 3 DS-GVO genannten Angaben.

(2) Der Auftragnehmer wird den Auftraggeber im Falle des § 4 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Informationen, Auskünfte und Nachweise zur Verfügung zu stellen, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten und zur Durchführung einer Kontrolle gemäß § 7 Abs. 1 dieses Vertrages erforderlich sind. Ferner wird der Auftragnehmer dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung stellen.

§ 5 Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DS-GVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO zu unterstützen.

(3) Der Auftragnehmer bestätigt, dass er –soweit eine gesetzliche Verpflichtung hierzu besteht- einen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten sind _____ _____.
Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

(4) Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegt.

§ 6 Subunternehmerverhältnisse

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern ("**Subunternehmerverhältnis**") befugt. Ausnahmen sind nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers im Einzelfall zulässig; bei Vertragsschluss erstreckt sich die Zustimmung des Auftraggebers auf die in **Anlage 4** genannten Subunternehmer des Auftragnehmers. In diesem Fall hat der Auftragnehmer dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den von ihm beauftragten Subunternehmen gelten, wobei dem Auftraggeber gegenüber dem Subunternehmer sämtliche Kontrollrechte gemäß § 7 dieses Vertrages einzuräumen sind. Subunternehmerverhältnisse zu Dritten außerhalb des Europäischen Wirtschaftsraumes sind nur gestattet, soweit für das betreffende Drittland ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören zB Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 7 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 3 Abs. 3 dieser Vereinbarung, zu überzeugen. Hierfür kann er zB Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig. Der Auftraggeber ist zu Kontrollen ohne vorherige Verständigung bzw. Anmeldung berechtigt, wenn andernfalls der Kontrollzweck gefährdet wäre.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DS-GVO. Er wird dem Auftraggeber unverzüglich, spätestens aber innerhalb von 5 Werktagen, die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftragnehmer nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DS-GVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich, spätestens binnen einer Frist von 5 Werktagen zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

§ 9 Laufzeit und Kündigung

(1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

(2) Der Auftraggeber ist jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer zunächst eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Auftraggeber sodann das Recht zur außerordentlichen Kündigung zu.

(3) Sollte eine Auftragsbeendigung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieses Vertrages bis zum tatsächlichen Ende der Verarbeitung.

§ 10 Löschung und Rückgabe

(1) Der Auftragnehmer wird dem Auftraggeber jederzeit auf dessen Verlangen sowie in jedem Fall nach Abschluss der Erbringung der Verarbeitungsleistungen alle ihm überlassenen Unterlagen, Daten und Datenträger nach Wahl des Auftraggebers zurückgeben oder, sofern nicht eine den Auftragnehmer bindende Aufbewahrungsfrist nach dem Recht der Europäischen Union oder eines Mitgliedsstaats besteht,

vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen dürfen keine personenbezogenen Daten mehr enthalten, sind vom Auftragsnehmer für eine Dauer von 3 Jahren aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

(2) Der Auftragnehmer wird dem Auftraggeber die Löschung schriftlich bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren; § 7 Abs. 2 dieses Vertrags gilt hierfür entsprechend.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. § 11 Abs. 2 Satz 1 gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 12 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Hamm.

_____, den ___.___._____

_____

Auftragnehmer

Hamm, den ___.___._____

_____

Stadt Hamm

Anlagen

Anlage 1 – Beschreibung der Datenarten und Kategorien betroffener Personen sowie Konkretisierung von Art und Zweck der Datenverarbeitung

Anlage 2 – Weisungs- und empfangsberechtige Personen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DS-GVO)

Anlage 4 – Bei Vertragsschluss zugelassene Subunternehmer des Auftragnehmers

Anlage 1

Beschreibung der Datenarten und Kategorien betroffener Personen sowie Konkretisierung von Art und Zweck der Datenverarbeitung

Datenarten	**Kategorien betroffener Personen**	**Art der Datenverarbeitung**	**Zweck der Datenverarbeitung**
z.B.: Personenstammdaten (Name, Vorname, Geburtsdatum, Sozialversicherungsnummer, Steuernummer) Kommunikationsdaten (zB Adresse, Telefon, E-Mail) Gehaltsdaten Versicherungsdaten Buchhaltungsdaten Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie Vertragsabrechnungs- und Zahlungsdaten Planungs- und Steuerungsdaten Auskunftsangaben (von Dritten, zB Auskunfteien, oder aus öffentlichen Verzeichnissen)	z.B.: Kunden Interessenten Abonnenten Mitarbeiter/Beschäftigte Lieferanten Handelsvertreter Ansprechpartner	Ergibt sich aus Gegenstand und Zweck der Datenverarbeitung	Möglichst konkrete Beschreibung des mit der Datenverarbeitung im Rahmen des Auftragsverarbeitungsverhältnisses verfolgten Zieles

Anlage 2

Weisungs- und empfangsberechtige Personen

1. Weisungsberechtigte Personen des Auftraggebers

Name, Vorname	Organisationseinheit	Kontaktdaten (Telefon, E-Mail)

2. Empfangsberechtigte Personen des Auftragnehmers

Name, Vorname	Organisationseinheit	Kontaktdaten (Telefon, E-Mail)

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DS-GVO)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

→ Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Beispiele für technische Maßnahmen: Alarmanlage, automatisches Zugangskontrollsystem, biometrische Zugangssperren, Chipkarten/Transpondersysteme, manuelles Schließsystem, Sicherheitsschlösser, Schließsystem mit Codesperre, Absicherung der Gebäudeschächte, Türen mit Knauf Außenseite, Klingelanlage mit Kamera, Videoüberwachung der Eingänge

Beispiele für organisatorische Maßnahmen: Schlüsselregelung/Liste, Empfang/Rezeption/Pförtner, Besucherbuch/Protokoll der Besucher, Mitarbeiter-/Besucherausweise, Besucher in Begleitung durch Mitarbeiter, Sorgfalt bei Auswahl des Wachpersonals, Sorgfalt bei Auswahl der Reinigungsdienste

b) Zugangskontrolle

→ Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Beispiele für technische Maßnahmen: Login mit Benutzername + Passwort, Zwei-Faktor-Authentifizierung, Login mit biometrischen Daten, Anti-Viren-Software Server, Anti-Viren-Software Clients, Anti-Viren-Software mobile Geräte, Firewall, Intrusion Detection Systeme, Mobile Device Management, Einsatz VPN bei Remote-Zugriffen, Verschlüsselung von Datenträgern, Verschlüsselung Smartphones, Gehäuseverriegelung, BIOS Schutz (separates Passwort), Sperre externer Schnittstellen (USB), automatische Desktopsperre, Verschlüsselung von Notebooks/Tablets

Beispiele für organisatorische Maßnahmen: Erstellen von Benutzerprofilen, zentrale Passwortvergabe, Richtlinie „Sicheres Passwort“, Richtlinie „Löschen/Vernichten“, Richtlinie „Clean Desk“, Allgemeine Richtlinie Datenschutz und/oder Sicherheit, Mobile Device Policy, Anleitung „Manuelle Desktopsperre“

c) Zugriffskontrolle

→ Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Beispiele für technische Maßnahmen: Aktenschredder (mind. Stufe 3, cross cut), externer Aktenvernichter (DIN 32757), physische Löschung von Datenträgern, Protokollierung von Zugriffen auf Anwendungen - konkret bei der Eingabe, Änderung und Löschung von Daten

Beispiele für organisatorische Maßnahmen: Einsatz Berechtigungskonzepte, bedarfsgerechte Zugriffsrechte, minimale Anzahl an Administratoren, Datenschutztresor, Verwaltung Benutzerrechte durch Administratoren, bei Online-Zugriffen des Auftraggebers: Zuständigkeit für die Ausgabe und Verwaltung von Zugriffssicherungscodes

d) Trennungskontrolle

→ Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Beispiele für technische Maßnahmen: Trennung von Produktiv- und Testumgebung (Sandboxing), physikalische Trennung (Systeme/Datenbanken/Datenträger), Mandantenfähigkeit relevanter Anwendungen

Beispiele für organisatorische Maßnahmen: Steuerung über Berechtigungskonzept, Festlegung von Datenbankrechten, Datensätze sind mit Zweckattributen versehen

e) Pseudonymisierung, Datenminimierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

→ ggf. 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 technischen und organisatorischen Maßnahmen unterliegen

→ ggf. weitere Maßnahmen zur Datenminimierung

Beispiele für technische Maßnahmen: im Falle der Pseudonymisierung Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)

Beispiele für organisatorische Maßnahmen: interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

→ Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Beispiele für technische Maßnahmen: Identifizierung und Authentifizierung, E-Mail-Verschlüsselung, Einsatz von VPN, Protokollierung der Zugriffe und Abrufe, sichere Transportbehälter, Bereitstellung über verschlüsselte Verbindungen wie sftp, https, Nutzung von Signaturverfahren, automatischer Rückruf

Beispiele für organisatorische Maßnahmen: Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen, Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge, Weitergabe in anonymisierter oder pseudonymisierter Form, Sorgfalt bei der Auswahl von Transportpersonal und -fahrzeugen, persönliche Übergabe mit Protokoll

b) Eingabekontrolle

→ Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Beispiele für technische Maßnahmen: technische Protokollierung der Eingabe, Änderung und Löschung von Daten, manuelle oder automatisierte Kontrolle der Protokolle

Beispiele für organisatorische Maßnahmen: Dokumentenmanagement, Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen), Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes, Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden, klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Verfügbarkeitskontrolle

→ Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Beispiele für technische Maßnahmen: Feuer- und Rauchmeldeanlagen, Feuerlöscher Serverraum, Serverraumüberwachung Temperatur und Feuchtigkeit, Serverraum klimatisiert, unterbrechungsfreie Stromversorgung (USV), Schutzsteckdosenleisten Serverraum, Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.), RAID System/Festplattenspiegelung, Videoüberwachung Serverraum, Alarmmeldung bei unberechtigtem Zutritt zu Serverraum, Virenschutz/Firewall

Beispiele für organisatorische Maßnahmen: Backup & Recovery-Konzept (ausformuliert: online/offline; on-site/off-site; Rhythmus, Medium, Aufbewahrungszeit, Aufbewahrungsort), Kontrolle des Sicherungsvorganges, regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse, Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraumes, keine sanitären Anschlüsse im/oberhalb des Serverraumes, Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4), Festlegung von Meldewegen, getrennte Partitionen für Betriebssysteme und Daten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

→ Maßnahmen zur Sicherstellung eines technisch und organisatorisch angemessenen Standes bei der Erbringung der vertraglich vereinbarten Leistungen

a) Datenschutz-Management

Beispiele für technische Maßnahmen: Software-Lösungen für Datenschutz-Management im Einsatz, zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z.B. Wiki, Intranet …), Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12, anderweitiges dokumentiertes Sicherheitskonzept, mindestens jährliche Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen

Beispiel für organisatorische Maßnahmen: interner/externer Datenschutzbeauftragter (Name, Firma, Kontaktdaten), Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet, regelmäßige (mindestens jährliche) Sensibilisierung der Mitarbeiter, interner/externer Informationssicherheitsbeauftragter (Name, Firma, Kontakt), Datenschutzfolgeabschätzung (DSFA) wird bei Bedarf durchgeführt,

Informationspflichten nach Art. 13 und 14 DSGVO wird nachgekommen, formalisierter Prozess zur Bearbeitung von Auskunftsanfragen Betroffener vorhanden

b) Incident-Response-Management

→ Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Beispiele für technische Maßnahmen: Einsatz von Firewall und regelmäßige Aktualisierung, Einsatz von Spamfilter und regelmäßige Aktualisierung, Intrusion Detection System (IDS), Intrusion Prevention System (IPS)

Beispiele für organisatorische Maßnahmen: dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde), dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen, Einbindung von Datenschutzbeauftragten und/oder Informationssicherheitsbeauftragten in Sicherheitsvorfälle und Datenpannen, Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem, formaler Prozess und Verantwortlichkeit zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

→ Privacy by design/Privacy by default

Beispiele für technische Maßnahmen: es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind, einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen

d) Auftragskontrolle (Outsourcing an Dritte)

→ Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Beispiele für organisatorische Maßnahmen: formalisiertes Auftragsmanagement, vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation, Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit), Abschluss der notwendigen und eindeutig ausgestalteten Vereinbarung zur Auftragsverarbeitung, schriftliche Weisungen an den Auftragnehmer, Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis, Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer (bei Bestellpflicht), Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer, Regelung zum Einsatz weiterer Subunternehmer, Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, bei längerer Zusammenarbeit: laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anlage 4

Bei Vertragsschluss zugelassene Subunternehmer des Auftragnehmers

Name, Rechtsform	**Ladungsfähige Anschrift, Kontaktdaten**	**Leistungsbeschreibung**
		kurze Beschreibung des Aufgabenbereichs, die Aufgabenbereiche mehrerer Unterauftragnehmer sind eindeutig abzugrenzen