

Vertrag zur Auftragsverarbeitung

zwischen der

Dortmunder Energie- und Wasserversorgung GmbH
Günter-Samtlebe-Platz 1
44135 Dortmund

- nachstehend **Auftraggeber** genannt –

und der

Muster GmbH
Muster-Str. 9
Musterstadt

- nachstehend **Auftragnehmer** genannt -

gemäß Art. 28 DS-GVO.

1. Gegenstand und Dauer des Vertrags

(1) Gegenstand

- ☒ Der Gegenstand des Vertrags ergibt sich aus der Leistungsvereinbarung/SLA/, auf die hier verwiesen wird.
- ☐ Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: (Bitte Beschreibung der Aufgaben hier eintragen)

(2) Dauer

- ☒ Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.
- ☐ Der Vertrag beinhaltet eine einmalige Ausführung.
- ☐ Die Dauer dieses Vertrags (Laufzeit) ist befristet bis zum (Datum).

- ☐ Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von (Datum) zum (Datum) gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Vertragsinhalts

(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 (siehe Punkt 1.1).
- ☐ Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: (Bitte Beschreibung des Vertragsgegenstands hier eintragen).

(2) Art der Daten

- ☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: (siehe Punkt 1.1)
- ☒ 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
 - ☐ Auskunftsangaben (von Dritten, z. B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
 - ☒ IT-Nutzungsdaten (Benutzerkennungen, IP-Adressen, Gerätenamen, Log-Files)
 - ☒ Inhaltsdaten (Ticketbeschreibungen, Anhänge, Screenshots, ggf. Fernwartungsprotokolle)

(3) Kategorien betroffener Personen

- ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: (siehe Punkt 1.1)
- ☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
 - ☐ Kunden
 - ☐ Interessenten
 - ☐ Abonnenten
 - ☒ Beschäftigte
 - ☐ Lieferanten
 - ☐ Handelsvertreter
 - ☐ Ansprechpartner
 - ☐ (bei Bedarf zusätzliche hinzufügen)

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 Vertrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1 und Abs. 2 DS-GVO 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, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die dokumentierten Maßnahmen sind in **Anlage x** aufzuführen und werden Grundlage des Vertrags.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und so weit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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 Löschkonzepte, die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung, sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO 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, Anschrift, 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, Anschrift, 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, Anschrift, Telefon, E-Mail].

- d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 berechtigterweise 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.
- e) Die Umsetzung und Einhaltung aller für diesen Vertrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Maßnahmen sind in **Anlage 2** aufgeführt).
- 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 Vertrag 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.
- i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrags.
- j) 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.
- k) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

- l) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.
- m) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

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 in Anspruch nimmt, z. B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu:

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

- c) ☒ die Auslagerung auf Unterauftragnehmer oder
- d) ☒ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:
 - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in eine angemessene Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
 - 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 Art. 28 Abs. 2-4 DS-GVO 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. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(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. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

☒ 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.

☐ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland (z. B. USA, Großbritannien). Das angemessene Schutzniveau

- ☐ 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 (Art. 46 Abs. 2 lit. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i. V. m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i. V. m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: (die Maßnahmen ausführlich beschreiben) (Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DS-GVO)

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. 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 Art. 28 DS-GVO 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.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten 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-Folgeabschätzung;
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

10. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(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.

(3) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer unverzüglich/zeitnahe in Textform mitteilen.

(4) Der Auftragnehmer kann dem Auftraggeber Personen oder Funktionen (z. B. Abteilungen etc.) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen oder Funktionen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen oder Funktionen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen. Der Auftraggeber behält sich das Recht vor im Zuge einer solchen Änderung die **Anlage 1** entsprechend anzupassen und diese dem Vertrag beizufügen.

11. Löschung und Rückgabe von personenbezogenen Daten

(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 Auftragsverarbeitung und der 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.

12. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Sollten einzelne Teile dieses Vertrags unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrags nicht. Die Parteien verpflichten sich, in einem derartigen Fall eine wirksame oder durchführbare Bestimmung an die Stelle der unwirksamen oder undurchführbaren zu setzen, die dem Geist und dem Zweck der zu ersetzenden Bestimmung soweit als möglich entspricht; dasselbe gilt für etwaige Lücken im Vertrag.

(3) Gerichtsstand ist Dortmund (für die einzelnen 21GRUPPE Unternehmen jeweils der im Handelsregister eingetragene Firmensitz).

Dortmund _____, den _____
Ort Datum

- Auftraggeber -

- Auftragnehmer -

Anlage 1 – Weisungsberechtigte Personen

1. Ansprechpartner und Weisungsberechtigte seitens Auftraggeber

Name	Kontaktdaten	Funktion

2. Ansprechpartner und Weisungsempfänger seitens Auftragnehmer

Name	Kontaktdaten	Funktion

Anlage 2 – Sicherheit der Verarbeitung (Technisch-organisatorische Maßnahmen)

Zutrittskontrolle

(Räume und Gebäude)

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.

Zusätzliche Bemerkungen:

- ☐ Zäune
- ☐ Personenkontrolle beim Pförtner/Empfang
- ☐ Automatisches Zutrittskontrollsystem/Vereinzelungsanlage
- ☐ Videoüberwachung
- ☐ Absicherung von Gebäudeschächten
- ☐ Sicherheitsverglasung
- ☐ Sicherheitsschlösser
- ☐ Schließsystem mit Codesperre
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Einteilung in Sicherheitszonen/Sperrbereiche
- ☐ Alarmanlage
- ☐ Manuelles Schließsystem
- ☐ Biometrische Zutrittssperren
- ☐ Lichtschranken/Bewegungsmelder
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Schriftliche Zutrittsregelungen (für berechnigte, nicht berechnigte Mitarbeiter und unternehmensfremde Personen)
- ☐ Protokollierung und Begleitung von Besuchern
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Tragepflicht von Berechnigungsausweisen
- ☐ Zutrittskontrolle bei Telearbeit/Mobiler Arbeit geregelt
- ☐ Sonstige Maßnahmen

Zugangskontrolle

(IT-Systeme, Anwendungen)

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Zusätzliche Bemerkungen:

- ☐ Zuordnung von Benutzerrechten
- ☐ Erstellen von Benutzerprofilen
- ☐ Passwortregelungen (Länge, Zusammensetzung, Wechsel)
- ☐ Protokollierung der Passwortnutzung
- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Automatische Bildschirmsperre
- ☐ Zugangssperre bei x Fehlversuchen
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Gehäuseverriegelungen
- ☐ Einsatz von VPN-Technologie
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Einsatz von Intrusion-Detection-Systemen (Abwehr von Angriffen von außen)
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum externen Löschen von Daten)
- ☐ Einsatz von Anti-Viren-Software
- ☐ Verschlüsselung von Datenträgern in Laptops/Notebooks
- ☐ Einsatz einer Hardware-Firewall
- ☐ Einsatz einer Software-Firewall

Zugriffskontrolle

(auf Daten)

Es ist zu 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.

Zusätzliche Bemerkungen:

- ☐ Erstellen eines Berechtigungskonzepts
- ☐ Zertifikatsbasierte Zugriffsberechtigung
- ☐ Verwaltung der Rechte durch Systemadministrator
- ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Datenträgerverwaltung
- ☐ Physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Ordnungsgemäße Vernichtung von Datenträgern
- ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☐ Protokollierung der Vernichtung
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern

Eingabekontrolle

(in Datenverarbeitungssysteme)

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.

Zusätzliche Bemerkungen:

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Aufbewahrung und Löschung der Protokolle
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Weitergabekontrolle

Es ist zu 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.

Zusätzliche Bemerkungen:

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ E-Mail-Verschlüsselung
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen, Verschlüsselung abhängig vom Schutzniveau
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen je nach Schutzniveau
- ☐ Regelung „Bring your own Device“
- ☐ Vollständigkeits- und Richtigkeitsprüfung (z. B. Plausibilität oder Checksumme)

Verfügbarkeitskontrolle

(von Daten)

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Zusätzliche Bemerkungen:

- ☐ Unterbrechungsfreie Stromversorgung (USV) und USV Test
- ☐ Überspannungsschutz
- ☐ Klimaanlage in Serverräumen
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Erstellen eines Backup- & Recoverykonzeptes (RAID, Festplattenspiegelung etc.)
- ☐ Testen von Datenwiederherstellung
- ☐ Erstellen eines Notfallplans
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Serverräume nicht unter sanitären Anlagen
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze

Datentrennung

(zweckbezogen)

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Zusätzliche Bemerkungen:

- ☐ Getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Getrennte Datensicherung
- ☐ Logische Mandantentrennung
- ☐ Erstellung eines Berechtigungskonzepts (z. B. werden unterschiedliche Mandanten von unterschiedlichen MA des AN verarbeitet)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☐ Festlegung von Datenbankrechten
- ☐ Trennung von Produktiv- und Testsystem

Auftragsdatenverarbeitung

(beim Einsatz von Subunternehmern)

Es ist zu gewährleisten, dass beim Einsatz von Subunternehmern durch den Auftragnehmer die Vorgaben des Auftraggebers umgesetzt werden.

Zusätzliche Bemerkungen:

- ☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☐ Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☐ schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag)
- ☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit und Verschwiegenheit
- ☐ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- ☐ Vertragsstrafen bei Verstößen
- Schulung der Mitarbeitenden zur Informationssicherheit und/oder Datenschutz