STADT BOCHUM

Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO (Anhang 06)

Vereinbarung

zwischen der

Stadt Bochum
Willy-Brandt-Platz 2-6
44777 Bochum

- Auftraggeber - nachstehend Stadt Bochum genannt -

und

Wählen Sie ein Element aus.

Klicken Sie hier, um Text einzugeben.

- Auftragsverarbeiter -

Hinweise

„Auftragsverarbeiter“ ist gem. Art. 4 Ziffer 8 EU-DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Die einzelnen Festlegungen nach Art. 28 Abs. 3 EU-DSGVO 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.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Der Gegenstand des Auftrags ergibt sich aus der Detaillierten Leistungsbeschreibung zur Auswahl und Einführung eines verwaltungsweiten Identity & Access Management Tools mit Zuschlagserteilung.

mit der Vertragsnummer **StBo_ZVS1_2026_00542_OV_IT,**

auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“).

☐ Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter: …

(2) Dauer

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung
☐ Der Auftrag wird zur einmaligen Ausführung erteilt
☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum Datum
☐ 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 Auftragsverarbeiter für die Stadt Bochum sind konkret beschrieben in der o. g. Leistungsvereinbarung.

Die Speicherung von personenbezogenen Daten (Data at Rest) erfolgt innerhalb der EU und des EWR sowie, sofern ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO besteht, in der Schweiz. Soweit ein Datentransfer personenbezogener Daten in Drittstaaten stattfindet (z. B. von personenbezogenen Metadaten), ist der Transfer nur zulässig, sofern die in Kapitel 5 der DSGVO niedergelegten Bedingungen eingehalten werden.

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: …
☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
  ☒ Personenstammdaten
  ☒ Kommunikationsdaten (z. B. Telefon, E-Mail)
  ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  ☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien oder aus öffentl. Verzeichnissen)
☐ …

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: …
☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
☐ Kunden
☐ Interessenten
☐ Abonnenten
☒ Beschäftigte
☐ Lieferanten
☐ Handelsvertreter
☐ Ansprechpartner
☒ externe Mitarbeitende

(4) Schutzbedarf

(a) Der Schutzbedarf für die Anwendung ist

☐ normal

☒ hoch (ergänzende Risikoanalyse auf gesondertem Blatt erforderlich, wird nach Zuschlagserteilung bereitgestellt)

☐ sehr hoch (ergänzende Risikoanalyse auf gesondertem Blatt erforderlich)

Begründung: siehe beigefügte Risikoanalyse

(b) Der Auftragsverarbeiter hat während der gesamten Dauer der Auftragsverarbeitung die in der Anlage 1 zu dieser Vereinbarung festgelegten technischen und organisatorischen Maßnahmen einzuhalten.

3. Weisungen der Stadt Bochum

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Stadt Bochum verarbeiten. Die Stadt Bochum entscheidet im Innenverhältnis zwischen den Parteien allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragsverarbeiters, ist nicht zulässig
(2) Dies gilt nicht, wenn der Auftragsverarbeiter nach dem Recht der EU oder des Mitgliedsstaats der EU, dessen Recht für ihn gilt, zu einer Datenverarbeitung verpflichtet ist. Liegt ein solcher Fall einer von Weisungen unabhängigen und/oder ihnen widersprechenden Verarbeitung personenbezogener Daten vor, teilt der Auftragsverarbeiter der Stadt Bochum diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, eine solche Mitteilung ist ebenfalls verboten.
(3) Mündliche Weisungen werden unverzüglich textlich (mind. per E-Mail) bestätigt.

(4) Der Auftragsverarbeiter hat die Stadt Bochum unverzüglich unter Angaben von Gründen zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Hält der Auftragsverarbeiter Weisungen des Dritten gem. Abs. 1 S. 3 für rechtswidrig, informiert er den Dritten unmittelbar darüber und unterrichtet die Stadt Bochum über den Vorgang. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Stadt Bochum oder den Dritten bestätigt oder geändert wird.

(5) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der Stadt Bochum unmittelbar durch den Auftragsverarbeiter sicherzustellen.

(6) Weisungsberechtigte Personen der Stadt Bochum sind

1: Jonas Kirchner, 11 IT 11 Server, Verfahrensbetreuer

2: tba

Weisungsempfänger beim Auftragsverarbeiter sind in der o. g. Leistungsvereinbarung aufgeführt oder Name, Vorname, Funktion.

Die Stadt Bochum kann jede weisungsberechtigte Person, der Auftragsverarbeiter jede(n) Weisungsempfänger(in) jederzeit abberufen oder neuberufen. Ab- bzw. Neuberufungen sind gegenüber dem Vertragspartner nur wirksam, wenn sie ihm in Textform mitgeteilt werden. Weisungen, die vor Zugang dieser Mitteilung vom oder gegenüber dem abberufenen Weisungsberechtigten bzw. dem neu berufenen Weisungsempfänger erteilt wurden, sind wirksam.

4. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe mit der Stadt Bochum vereinbarten erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und der Stadt Bochum zur Prüfung zu übergeben. Die umzusetzenden technischen und organisatorischen Maßnahmen sind in der Anlage 1 zu diesem Vertrag dargestellt. Soweit die Prüfung/ ein Audit der Stadt Bochum einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO 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 EU-DSGVO zu berücksichtigen. Das erforderliche Schutzniveau ergibt sich aus Nr. 2 (4). Ist dort nichts geregelt, ist es gesondert festzulegen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Darüber hinaus beobachtet der Auftragsverarbeiter die technische Entwicklung und schlägt ggf. notwendige Anpassungen der technisch-organisatorischen Maßnahmen vor.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) ☒ Der Auftragsverarbeiter wird schriftlich einen Datenschutzbeauftragten bestellen, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt. Dessen Kontaktdaten werden der
Stadt Bochum zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird der Stadt Bochum unverzüglich mitgeteilt.

☐ Als Datenschutzbeauftragte/r ist beim Auftragsverarbeiter … bestellt. Ein Wechsel des Datenschutzbeauftragten ist der Stadt Bochum unverzüglich mitzuteilen.

☐ Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt.

☐ Der Auftragsverarbeiter ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragsverarbeiter wird … benannt.

☐ Da der Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 EU-DSGVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

(2) Der Auftragsverarbeiter verpflichtet sich, die ihm im Rahmen des Auftragsverhältnisses zur Verfügung gestellten oder erarbeiteten Unterlagen und Daten sowie ihm sonst bekannt gewordene Informationen vertraulich zu behandeln und nur im Rahmen der Tätigkeit für dieses Vertragsverhältnis zu nutzen. Diese Verpflichtung gilt auch nach Ende des Vertragsverhältnisses auf unbegrenzte Zeit fort. Der Auftragsverarbeiter 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 Auftragsverarbeiter belehrt die bei der Durchführung der Arbeiten eingesetzten Personen insbesondere darüber, dass sie Daten nur auf Weisung der Stadt Bochum verarbeiten dürfen, wenn sie gesetzlich nicht zu einer anderen Verarbeitung verpflichtet sind. Er überwacht durch regelmäßige Kontrollen, dass sie diese Verpflichtung einhalten. Er unterrichtet sie regelmäßig über ihre datenschutzrechtlichen Verpflichtungen und deren Wirksamkeit.

(3) Der Auftragsverarbeiter setzt alle für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO um und hält sie ein.

(4) Die Stadt Bochum und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Der Auftragsverarbeiter informiert den die Stadt Bochum unverzüglich 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 Auftragsverarbeiter ermittelt.

(6) Soweit die Stadt Bochum ihrerseits 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

(7) Der Auftragsverarbeiter weist die getroffenen technischen und organisatorischen Maßnahmen gegenüber der Stadt Bochum nach.
(8) Der Auftragsverarbeiter unterstützt die Stadt Bochum vollumfänglich durch geeignete Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der Betroffenen. Soweit eine betroffene Person sich in Ausübung ihrer Rechte unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an die Stadt Bochum weiterleiten.
(9) Der Auftragsverarbeiter übernimmt noch weitere Verpflichtungen auf Grund weiterer datenschutzrechtlicher Normen wie folgt:

6. Unterauftragsverhältnisse

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

☒ Der Auftragsverarbeiter darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung der Stadt Bochum beauftragen. Er hat dem Unterauftragsverarbeiter dieselben Regelungen aufzuerlegen, die dem Auftragsverarbeiter nach diesem Vertrag auferlegt wurden. Die Zustimmung der Stadt Bochum gilt als erteilt, wenn der Auftragsverarbeiter die entsprechenden Unterauftragsverarbeiter und den jeweiligen Umfang der Unterauftragsverarbeitung in seinem Angebot benannt bzw. dargelegt hat.

☐ Eine Unterbeauftragung ist unzulässig.

☐ Die Stadt Bochum stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO:

Firma/ Unterauftragsverarbeiter	Anschrift/Land	Leistung

☐ Die Auslagerung auf Unterauftragsverarbeiter und/oder

☐ der Wechsel des bestehenden Unterauftragsverarbeiters

ist/sind zulässig, soweit:

(a) der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragsverarbeiter der Stadt Bochum mit einer Vorlaufzeit von vier Wochen schriftlich oder in Textform anzeigt und

(b) die Stadt Bochum nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
(c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

(2) Die Weitergabe von personenbezogenen Daten der Stadt Bochum an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

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

(4) Eine weitere Auslagerung durch den Unterauftragsverarbeiter

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung der Stadt Bochum (mind. Textform). Diese gilt als erteilt, wenn der Auftragsverarbeiter die entsprechenden Unterauftragsverarbeiter und den jeweiligen Umfang der Unterauftragsverarbeitung in seinem Angebot benannt bzw. dargelegt hat.

☐ bedarf der ausdrücklichen Zustimmung des Dritten (mind. Textform).

Die Stadt Bochum ist vor der Zustimmung über die geplante Auftragsvergabe an den Unterauftragsverarbeiter so zu unterrichten, dass er dazu Stellung nehmen kann. Die Stadt Bochum ist ferner über die erteilte Zustimmung zu unterrichten.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

7. Kontrollrechte der Stadt Bochum

(1) Die Stadt Bochum hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch von ihm beauftragte Prüfer durchführen zu lassen. Er hat das Recht, sich durch Kontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung, der Vorschriften der DSGVO und weiterer evtl. einschlägiger datenschutzrechtlicher Vorschriften durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter unterstützt die Stadt Bochum bei diesen Prüfungen. Ggf. sorgt der Auftragsverarbeiter auch dafür, dass die Stadt Bochum oder von ihm beauftragte Prüfer Prüfungen auch bei Unterauftragsverarbeitern durchführen können und auch diese die Stadt Bochum bzw. dessen Prüfer unterstützen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich die Stadt Bochum von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, der Stadt Bochum 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 EU-DSGVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;

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

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

8. Mitwirkung des Auftragsverarbeiters bei der Erfüllung der Pflichten nach Art. 32 ff. DSGVO

(1) Der Auftragsverarbeiter unterstützt die Stadt Bochum und –bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen 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 des Schutzes personenbezogener Daten unverzüglich an die Stadt Bochum zu melden
(c) die Verpflichtung, die Stadt Bochum im Rahmen ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
(d) die Unterstützung der Stadt Bochum für dessen Datenschutz-Folgenabschätzung
(e) die Unterstützung der Stadt Bochum im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen der Stadt Bochum 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 die Stadt Bochum – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Stadt Bochum 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 Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen

über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende der Stadt Bochum übergeben.

10. Außerordentliche Kündigung

Unabhängig von den Regelungen über die oben getroffenen Laufzeiten bzw. die Dauer der Vereinbarung steht der Stadt Bochum ein Recht auf fristlose Kündigung bei schwerwiegenden Vertragsverletzungen des Auftragsverarbeiters zu. Dies kommt insbesondere in Betracht bei Verstoß gegen datenschutzrechtliche Vorschriften, Datenschutz- und Datensicherheitsvereinbarungen, wenn der Auftragsverarbeiter eine Weisung der Stadt Bochum nicht ausführen kann oder will oder der Auftragsverarbeiter eine Kontrolle der Stadt Bochum oder der nordrhein-westfälischen Datenschutzbeauftragten vertragswidrig verweigert.

11. Haftung

(1) Im Verhältnis zu den betroffenen Personen richtet sich die Haftung der Stadt Bochum und des Auftragsverarbeiter nach den gesetzlichen Vorschriften (Art. 82 DSGVO).

(2) Im Haftungsfall gem. Abs. 1 haftet der Auftragsverarbeiter im Innenverhältnis der Stadt Bochum gegenüber für Schäden, die dadurch entstehen, dass er selbst oder die von ihm nach Nr. 6 eingeschalteten Unterauftragsverarbeiter die ihnen obliegenden Pflichten nicht erfüllen (siehe Art. 82 Abs. 2 Satz 2 DSGVO). Er stellt die Stadt Bochum insoweit auch von sämtlichen Schadensersatzansprüchen frei, die die betroffenen Personen gegenüber diesem wegen der Verletzung von Datenschutzbestimmungen, insbesondere der DSGVO oder des BDSG oder einer ansonsten unzulässigen oder unrichtigen Datenverarbeitung auf Grund der Verletzung einer solchen Pflicht im Rahmen des Vertragsverhältnisses der Parteien oder dieser Vereinbarung zur Auftragsverarbeitung geltend machen. Der Auftragsverarbeiter ist jedoch berechtigt, nachzuweisen, dass der der betroffenen Person entstandene Schaden nicht durch eine Pflichtverletzung einer der bei ihm beschäftigten Personen oder eines von ihm nach Ziff. 6 eingeschalteten Unterauftragsverarbeiters schuldhaft verursacht wurde. Ein Entlastungsbeweis steht auch dem Auftraggeber zu.

(3) Können sowohl der Auftragsverarbeiter als auch die Stadt Bochum von einer betroffenen Person auf Schadensersatz wegen der Verletzung von Pflichten nach datenschutzrechtlichen Vorschriften in Anspruch genommen werden, bestimmt sich die Haftung der Parteien im Innenverhältnis danach, inwieweit und in welchem Umfang die jeweiligen Parteien den Schaden verursacht bzw. verschuldet haben. Jede Partei kann bei der jeweils anderen Partei bis zur Höhe des von dieser Partei verursachten Schadens Rückgriff nehmen, soweit sie an die betroffene Person einen über den eigenen Verursachungs- und Verschuldungsanteil hinausgehenden Beitrag geleistet hat. Der Erstattungsanspruch ist auf die Höhe begrenzt, in der die jeweilige Partei an den oder die Geschädigte/n mehr als den von ihr intern geschuldeten Schadensanteil geleistet hat.

12. Sonstiges

(1) Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragsverarbeiters auf diese Vereinbarung keine Anwendung finden.

(2) Diese Vereinbarung enthält alle vertraglichen Regelungen zwischen den Parteien. Nebenabreden können getroffen werden. Sie bedürfen der Schriftform.

(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich des Anspruchs auf Rückgabe der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Gerichtsstand ist, wenn in der o. g. Leistungsvereinbarung nichts anderes vereinbart ist, Bochum.

13. Wirksamkeit der Vereinbarung

Diese Vereinbarung bleibt auch bei rechtlicher Unwirksamkeit einzelner Punkte in seinen übrigen Teilen verbindlich. Unwirksame Bestimmungen sind von den Parteien durch wirksame zu ersetzen, die dem gewollten Zweck möglichst nahe kommen. Entsprechendes gilt im Falle einer Vertragslücke.

Anlage 1: Technisch-organisatorische Maßnahmen zur Sicherstellung der Datensicherheit

Bochum, Ort, Datum

Im Auftrag:

_____ _____

Stadt Bochum Auftragsverarbeiter

Technisch-organisatorische Maßnahmen zur Sicherstellung der Datensicherheit

Vertragsnummer der Leistungsvereinbarung: StBo_ZVS1_2026_00542_OV_IT

Der Auftragsverarbeiter hat während der gesamten Laufzeit dieses Vertrags zur Auftragsdatenverarbeitung folgende technisch-organisatorische Maßnahmen einzuhalten:

Erstellt von:	Klicken Sie hier, um Text einzugeben.	Erstellt am:	Klicken Sie hier, um ein Datum einzugeben.

	voll erfüllt	teilerfüllt	nicht erfüllt	entfällt	Bemerkung
Infrastruktur					
Verhaltensregelung Pfortendienst und Gebäudesicherung	☐	☐	☐	☐	

	voll erfüllt	teilerfüllt	nicht erfüllt	entfällt	Bemerkung
Regelung für Räume mit speziellen Zutrittsvoraussetzungen	☐	☐	☐	☐	
Regelungen für Überwachungseinrichtungen	☐	☐	☐	☐	
Berücksichtigung von Brandabschnitten für personenbezogene Daten	☐	☐	☐	☐	
Klicken Sie hier, um Text einzugeben.	☐	☐	☐	☐	
Organisation					
Zutrittsregelungen	☐	☐	☐	☐	
Regelungen für Schließanlage	☐	☐	☐	☐	
Regelungen für Schlüsselmanagement, Regelung für externe Schlüsselbesitzer	☐	☐	☐	☐	
Zugangsregelung/Personenbezogene Zugangsberechtigungen	☐	☐	☐	☐	
Stellenbeschreibungen mit DS-Aspekten (insb. Personen mit erweiterten Rechten, z. B.: Admin)	☐	☐	☐	☐	
Zugriffsregelungen / Berechtigungskonzept	☐	☐	☐	☐	
Regelung der Thematik „externe Mitarbeiter“	☐	☐	☐	☐	
Regelungen zur E-Mail-Nutzung	☐	☐	☐	☐	
Regelung zur Internet-Nutzung	☐	☐	☐	☐	
Regelungen zur Passwort-Verwendung	☐	☐	☐	☐	
Regelung zur Mobiltelefonbenutzung	☐	☐	☐	☐	
Beschreibung Netzwerkaufbau / Netzkonzept	☐	☐	☐	☐	
Beschreibung der IT-Arbeitsplätze	☐	☐	☐	☐	

	voll erfüllt	teilerfüllt	nicht erfüllt	entfällt	Bemerkung
Beschreibung der Serverlandschaft	☐	☐	☐	☐	
Regelung zur Datenlöschung	☐	☐	☐	☐	
Regelungen zur Datenträgerlagerung	☐	☐	☐	☐	
Regelung zur Datenträgerentsorgung	☐	☐	☐	☐	
Regelungen zu mobilen DV-Einrichtungen	☐	☐	☐	☐	
Verträge mit Unterauftragsverarbeiter	☐	☐	☐	☐	
Verträge zum Datenschutz beim Outsourcing	☐	☐	☐	☐	
Regelung von Wartungsarbeiten	☐	☐	☐	☐	
Regelung zur Datenübermittlung - intern/extern - nicht öffentliche Stellen	☐	☐	☐	☐	
Regelung zu - Testabläufen Hard- und Software - Hard- und Softwareeinführung - Hard- und Softwarenutzung - Hard- und Softwareänderung	☐	☐	☐	☐	
Personal					
Regelungen Schulungen - Hard- und Software - Datenschutz & IT-Sicherheit	☐	☐	☐	☐	
Verpflichtung von Beschäftigten nach unterschiedlichen Gesetzen	☐	☐	☐	☐	
Verpflichtung von Beschäftigten der Unterauftragsverarbeiter / Externen	☐	☐	☐	☐	
Hard- und Software					
Externe Schnittstellen	☐	☐	☐	☐	
Register für - Hard- und Software - Verfahren	☐	☐	☐	☐	

	voll erfüllt	teilerfüllt	nicht erfüllt	entfällt	Bemerkung
- Archive - Virenschutz					
Kommunikation					
Verträge zur Fernwartung	☐	☐	☐	☐	
Notfallvorsorge					
Regelung zur Thematik Notfallmanagement	☐	☐	☐	☐	
Regelungen zur Datensicherung	☐	☐	☐	☐	
Versicherungsverträge (EDV-, Brand-, Wasserschaden)	☐	☐	☐	☐	

Weitere Bemerkungen

Thema	Anmerkung
Klicken Sie hier, um Text einzugeben.	Klicken Sie hier, um Text einzugeben.

Ausfüllhinweise zu den technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit:

1	Voll erfüllt	Alle Maßnahmen nach BSI-Standard oder vergleichbar ISO 27001 wurden umgesetzt
2	Teilerfüllt	Die BSI-Maßnahmen der Stufe A oder analog vergleichbare nach ISO27001 sind essentiell für die Sicherheit und vorrangig umgesetzt.
3	Nicht erfüllt	Es sind keine oder nur teilweise BSI-Maßnahmen der Stufe A oder analog vergleichbare nach ISO27001 umgesetzt
4	Entfällt	Nach Prüfung der Voraussetzungen können Maßnahmen entfallen. Z. B. wenn bestimmte Produkte nicht in der angenommenen Ausprägung eingesetzt werden.

Infrastruktur	**Beispiele**
Verhaltensregelung Pfortendienst und Gebäudesicherung	Die Einrichtung eines Pförtnerdienstes hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Die Arbeitsbedingungen des Pförtners sind für die Aufgabenwahrnehmung geeignet auszugestalten. Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben dem Pförtner im Zusammenspiel mit weiteren Schutzmaßnahmen zukommt (z. B. Gebäudesicherung nach Dienst- oder Geschäftsschluss, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).
Regelung für Räume mit speziellen Zutrittsvoraussetzungen	Ein Rechenzentrum stellt eine wichtige zentrale Einheit und damit eine Funktionseinheit mit besonderen Anforderungen an den Schutz gegen unbefugten Zutritt dar. Regelungen zur Vergabe von Zutrittsberechtigungen – in Verbindung mit elektronischen und mechanischen Zutrittskontrollsystemen sind die unabdingbare Basis für den Schutz eines RZ gegen unbefugten Zutritt.
Regelungen für Überwachungseinrichtungen	Die Maßnahmen zur Außensicherung und Zutrittskontrolle können durch den Einsatz von Videotechnik ergänzt werden. Videoüberwachungsanlagen, ob eigenständig oder ergänzend zu anderen Sicherheitstechniken, werden zur Erreichung der Schutzziele eingesetzt.
Berücksichtigung von Brandabschnitten für personenbezogene Daten	Zur Verwirklichung eines effizienten Brandschutzes ist die Zusammenarbeit aller zuständigen Verfahrensbeteiligten notwendig. Hierunter fallen die Funktionen ● des Brandschutz-Beauftragten (Arbeitgeber ist für die Einhaltung der Brandschutzvorschriften verantwortlich), ● der Fachkraft für Arbeitssicherheit (in Deutschland erforderlich nach §§ 5, 6 Arbeitssicherheitsgesetz, diese ist zuständig für die Ausgestaltung des betrieblichen Brandschutzes) und

	• des Sicherheitsbeauftragten (in Deutschland erforderlich nach § 22 SGB VII, dieser hat ausführende Tätigkeiten, z. B. zur Verhütung von Arbeitsunfällen und Berufskrankheiten, und arbeitet der Fachkraft für Arbeitssicherheit zu).
Organisation	
Zutrittsregelungen	Wurde der Schutzbedarf der verschiedenen Arten von Räumen bestimmt? Wurde festgelegt, welche Zutrittsrechte an welche Personen im Rahmen ihrer Funktionen vergeben wurde? Ist die Dokumentation der Zutrittsberechtigungen aktuell? Umfasst sie alle schutzbedürftigen Räume? Ist die Begleitung externer Besucher sichergestellt?
Regelungen für Schließanlage	Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten.
Regelungen für Schlüsselmanagement	Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Bei der Rücknahme einer Zutrittsberechtigung muss die Rücknahme der Zutrittsmittel gewährleistet sein. Zusätzlich ist zu dokumentieren, welche Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen aufgetreten sind. Gründe für Konflikte können vorliegen, weil Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder auf Grund räumlicher Notwendigkeiten.
Zugangsregelung / personenbezogene Zugangsberechtigungen	Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Zugangsberechtigungen sollten möglichst restriktiv vergeben werden. Diese sind für jede nutzungsberechtigte Person auf Grund ihrer Funktion unter Beachtung der Funktionstrennung im Einzelnen festzulegen.
Stellenbeschreibungen mit DS-Aspekten (insb. Personen mit erweiterten Rechten, z. B.: Admin)	Für alle wesentlichen Aufgaben und Geschäftsprozesse in einer Institution sollten die Verantwortlichkeiten nachvollziehbar geregelt sein.
Zugriffsregelungen / Berechtigungskonzept	Regelungen für die Einrichtung von Benutzern / Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs. Hier stellen sich vor allem die Fragen:

	• Gibt es organisatorische Regelungen zur Einrichtung von Benutzern bzw. Benutzergruppen? • Gibt es ein Programm zur Einrichtung von Benutzern bzw. Benutzergruppen?
Regelung der Thematik „Externe Mitarbeiter“, z. B. auch Reinigungskräfte	Häufig wird in Behörden oder Unternehmen auf externe Unterstützung zurückgegriffen, falls die entsprechenden personellen Ressourcen nicht im eigenen Haus vorhanden sind. Fragen: • Werden externe Mitarbeiter mit längerfristigen Aufgaben auf die Einhaltung der einschlägigen Gesetze und Vorschriften verpflichtet? • Werden externe Mitarbeiter geregelt in ihre Aufgaben eingearbeitet und über bestehende Regelungen zur IT-Sicherheit unterrichtet? • Werden bei sämtlichen eingerichteten Zugangsberechtigungen die Zugriffsrechte bei Auftragsende entzogen bzw. gelöscht?
Regelungen zur E-Mail-Nutzung	• Sind Regelungen für die Nutzung der dienstlichen E-Mail vorhanden? • Ist die private Nutzung verboten? • Gibt es Vorgaben zur Verschlüsselung personenbezogener Daten?
Regelung zur Internet-Nutzung	• Wurden für die Nutzung des Internets alle erforderlichen Richtlinien festgelegt? • Sind die Richtlinien allen Benutzern des Internets bekannt?
Regelungen zur Passwort-Verwendung	• Gibt es klare Regelungen zum Passwortgebrauch und der Passwortgestaltung? • Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden? • Wird die Passwort-Güte kontrolliert? • Wird ein regelmäßiger Passwort-Wechsel erzwungen? • Sind alle Benutzer von IT-Systemen und Anwendungen mit einem Passwort ausgestattet?
Regelung zur Mobiltelefonnutzung (wenn für das Verfahren relevant)	• Existiert eine aktuelle Sicherheitsrichtlinie für die Mobiltelefon-Nutzung? • Wie wird die Einhaltung der Sicherheitsrichtlinie für die Mobiltelefon-Nutzung überprüft? • Besitzt jeder Mobiltelefon-Benutzer ein Exemplar dieser Mobiltelefon-Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen? • Ist die Sicherheitsrichtlinie für die Mobiltelefon-Nutzung Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen? • Werden die Benutzer von Mobiltelefonen auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?

	• Werden die Benutzer von Mobiltelefonen auf die geeignete Aufbewahrung hingewiesen?
Transparenz / Beschreibung Netzwerkaufbau / Netzkonzept	Um den Anforderungen bezüglich Verfügbarkeit (auch Bandbreite und Performance), Vertraulichkeit und Integrität zu genügen, muss der Aufbau, die Änderung bzw. die Erweiterung eines Netzes sorgfältig geplant werden. Hierzu dient die Erstellung eines Netzkonzeptes.
Transparenz / Beschreibung der IT-Arbeitsplätze	• Existiert eine Richtlinie für die IT-Nutzung? • Wie wird die Einhaltung der Richtlinie überprüft? • Wird regelmäßig geprüft, ob die Inhalte der Richtlinie, insbesondere die einzuhaltenden IT-Sicherheitsmaßnahmen, noch aktuell sind? • Steht die Richtlinie für die IT-Nutzung jedem Benutzer zur Verfügung? • Wird die Richtlinie bei den Schulungen zu IT-Sicherheitsmaßnahmen berücksichtigt?
Transparenz / Beschreibung der Serverlandschaft	Eine grundlegende Voraussetzung dafür, dass ein Server sicher betrieben werden kann, ist ein angemessenes Maß an Planung im Vorfeld.
Regelung zur Datenlöschung	• Existiert eine datenschutzkonforme Richtlinie für die Löschung oder Vernichtung von Daten, Medien, Dokumenten, etc.? • Wird die Einhaltung der Richtlinie für die Löschung oder Vernichtung von Daten regelmäßig überprüft? • Ist die Richtlinie aktuell? Berücksichtigt sie alle zurzeit eingesetzten Datenträgerarten?
Regelungen zur Datenträgerlagerung	Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht.
Regelung zur Datenträgerentsorgung	• Ist die Entsorgung von schutzbedürftigen Materialien geregelt? • Ist sichergestellt, dass alle schutzbedürftigen Materialien ordnungsgemäß entsorgt werden?
Regelungen zu mobilen DV-Einrichtungen	• Existiert eine aktuelle Sicherheitsrichtlinie für die mobile Nutzung von IT-Systemen? • Ist jeder Benutzer von mobilen IT-Systemen darüber informiert, was die wichtigsten Sicherheitsmechanismen zu deren Schutz unterwegs sind? • Werden die Benutzer von mobilen IT-Systemen auf die Regelungen hingewiesen, die von ihnen einzuhalten sind? • Ist die Sicherheitsrichtlinie für die Nutzung von mobilen IT-Systemen Inhalt der Schulungen zu Sicherheitsmaßnahmen?

Verträge mit Unterauftragsverarbeitern	• Mit Unterauftragsverarbeitern sind Service Level Agreements (SLAs) abgeschlossen, die die Leistungstiefe und Qualität definieren. • In den SLAs sind Regelungen zur Informationssicherheit hinterlegt (Verpflichtung zu einem Sicherheitskonzept). • In den SLAs sind weitere Unterbeauftragungen seitens des Dienstleisters definiert.
Verträge zum Datenschutz beim Outsourcing	• Verträge mit Unterauftragsverarbeitern / Outsourcing-Partnern müssen eine Verpflichtung auf den Datenschutz enthalten (ggf. Details zu Technisch-Organisatorischen Maßnahmen). • Datenschutzprüfungen gegenüber Drittdienstleistern müssen sichergestellt sein.
Regelung von Wartungsarbeiten	Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde.
Regelung zur Datenübermittlung - intern / extern - nicht-öffentliche Stellen	Sind besondere gesetzliche Regelungen für die Datenübertragung zu beachten oder existieren hierzu eigene Arbeitsanweisungen (Sichere Netzzugangs- und Kommunikationstechnologien wie VPN mittels IPsec oder HTTPS, verschlüsselte Datenübertragungen, remote access, geregelter Transportprozess von Datensicherungsbändern, etc.)? Beispiel: • Allgemeine Verwaltungsvorschrift zur Datenübermittlung mit dem Verkehrszentralregister • Regelung der Datenübermittlung nach § 105 Abs. 2 SGB XI
Regelung zu - Testabläufen Hard- und Software - Hardwareeinführung - Softwareeinführung - Hardwarenutzung - Softwarenutzung - Hardwareänderung - Softwareänderung	Im Rahmen des Hard- und Software-Managements sind unabhängig von der Art der eingesetzten IT-Komponenten eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die für den sicheren Betrieb aller IT-Komponenten notwendigen Maßnahmen müssen in einer Sicherheitsrichtlinie festgelegt werden. Die Einhaltung des darin spezifizierten Sicherheitsniveaus, wie z. B. die Protokollierung benutzer- und systembezogener Aktivitäten, die revisionssichere Archivierung und der einheitliche Systemzeitabgleich, erfordert neben den technischen Maßnahmen auch ein umfangreiches Regelwerk für den Benutzer, das diesem Hilfestellung und eine verbindliche und präzise Anleitung gibt. Potentielle Risikofaktoren und Schwachstellen sind zum Beispiel: • Passwörter, • Fremdpersonal,

	• nicht freigegebene IT-Komponenten.
Personal	
Regelungen Schulungen - Hard- und Software - Datenschutz & IT-Sicherheit	• Werden die Mitarbeiter zu Themen rund um Datenschutz und Informationssicherheit geschult? • Werden neue Mitarbeiter in die Sicherheitsmaßnahmen eingewiesen? • Werden regelmäßig Schulungsmaßnahmen angeboten? • Werden Mitarbeiter, die eine Aufgabe neu übernehmen sollen, ausreichend geschult? • Werden die Administratoren spezifisch geschult?
Verpflichtung von Beschäftigten nach unterschiedlichen Gesetzen	• Werden die Mitarbeiter verpflichtet, alle bestehenden Gesetze, Vorschriften und Regelungen einzuhalten? • Ist den Mitarbeitern bekannt, welcher rechtliche Rahmen ihre Tätigkeit bestimmt?
Verpflichtung von Beschäftigten der Unterauftragsverarbeiter / Externen	• Werden Externe vor dem Zugang zu vertraulichen Informationen verpflichtet, diese vertraulich zu behandeln? • Werden durch die verwendeten Vertraulichkeitsvereinbarungen alle wichtigen Aspekte zum Schutz von organisationsinternen Informationen berücksichtigt?
Hard- und Software	
Externe Schnittstellen	• Ist der Zugriff auf Wechselmedien unterbunden oder reglementiert? • Sind die Benutzer über alle Regelungen zum Umgang mit Laufwerken für Wechselmedien und externen Datenspeicher informiert? • Ist sichergestellt, dass PCs nicht unkontrolliert von Wechselmedien gebootet werden können?
Register für - Hard- und Software - Verfahren - Archive	Neben den zentralen Datenverarbeitungsanlagen sind bei dezentraler Datenverarbeitung alle eingesetzten IT-Systeme zu erfassen. Es muss jederzeit auf ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten zugegriffen werden können.
Kommunikation	
Verträge zur Fernwartung	Wird vertraglich sowie technisch Folgendes sichergestellt: • Fernwartungszugriffe können immer nur vom lokalen IT-System initiiert werden. • Die Durchführung der Fernwartung wird ausreichend protokolliert.
Notfallvorsorge	

Regelung zur Thematik Notfallmanagement	Bestehen Übersichten und Regelungen zu: ● Notfallleitlinien und Notfallkonzepten ● Verfügbarkeitsanforderungen ● Definition eines Notfalls und Notfall-Verantwortlichen sowie der Verantwortung ● Alarmierungs- und Notfallpläne für ausgewählte Schadensereignisse sowie entsprechende Wiederanlaufpläne ● Ersatzbeschaffungen und Lieferantenvereinbarungen
Datensicherung	● Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Sind in einem Datensicherungskonzept Regelungen getroffen worden, welche Daten von wem wann gesichert werden? ● In diesem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat. Für eine ordnungsgemäße und funktionierende Datensicherung ist eine Dokumentation erforderlich.
Versicherungsverträge (EDV-, Brand- und Wasserschaden)	● Ist geprüft worden, ob für Restrisiken Versicherungen abgeschlossen werden sollen, um eventuelle Schäden abzudecken? ● Wurde der notwendige Versicherungsschutz ermittelt (u. a. Höhe der Versicherungssummen)? ● Wird regelmäßig überprüft, dass die bestehenden Versicherungen der aktuellen Lage entsprechen?

Ort, Datum	Bochum
	i.A.
_____	_____
Wählen Sie ein Element aus.	Stadt Bochum