

Ergänzungsvereinbarung

über die Verarbeitung personenbezogener Daten im Auftrag

**gemäß Art. 28 der Verordnung (EU) 2016/679
(Datenschutz-Grundverordnung, DS-GVO)**

zwischen der

- Verantwortlicher –

nachstehend „Auftraggeber“ genannt

und der/dem

.....

- Auftragsverarbeiter –

nachstehend „Auftragnehmer“ genannt.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

- ☒ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA
EVB-IT Systemvertrag vom
auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“).
- ☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: [Klicken Sie hier, um ein Datum einzugeben.](#)

(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 [Klicken Sie hier, um ein Datum einzugeben.](#)
- ☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von [Klicken Sie hier, um Text einzugeben.](#) zum [Klicken Sie hier, um Text einzugeben.](#) gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- ☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der o. g. Leistungsvereinbarung.
- ☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: im Störfall: Prüfung der Software zur Zusatzalarmierung auf Fehlern, Durchführung von Programmupdates.

(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 (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)
 - ☒ Einsatzdaten, welche aus dem Einsatzleitsystem übermittelt werden.

(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
 - ☒ Im Einsatz eingesetzte Einsatzkräfte und betroffene sowie beteiligte Personen.

(4) 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 Ort der Verarbeitung ist Deutschland. Jede Verlagerung in ein Drittland bedarf der vorherigen, schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Weisungen des Auftraggebers

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers verarbeiten. Der Auftraggeber entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragnehmers oder seines Unterauftragnehmers, ist nicht zulässig. Weisungen werden nur vom Auftraggeber und von keinem Dritten erteilt, auch wenn die Datenverarbeitung im Interesse oder Auftrag dieses Dritten erfolgt und/oder der Auftragnehmer Auftragsverarbeiter für diesen Dritten ist.

(2) Dies gilt nicht, wenn der Auftragnehmer 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 Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, eine solche Mitteilung ist ebenfalls verboten.

(3) Mündliche Weisungen des Auftraggebers bestätigt der Auftragnehmer unverzüglich textlich (mind. per Mail) und dokumentiert die Weisungen.

(4) Der Auftragnehmer hat den Auftraggeber unter Angaben von Gründen 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.

(5) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers im Namen des Auftragnehmers unmittelbar durch den Unterauftragnehmer sicherzustellen.

(6) Weisungsberechtigte Personen des Auftraggebers sind: Mitarbeiter der Fachstelle 37.22: Bexten, Ulrich; Hegemann, Christian; Knauer, Marc-Andre; Werner, Markus . Weisungsempfänger beim Auftragnehmer sind: Softwareentwicklung: Nieß, Michael, Servicetechniker: Winkels, Vincent.

4. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe mit dem Auftraggeber vereinbarten erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Die umzusetzenden technischen und organisatorischen Maßnahmen sind am Ende dieses Vertrags dargestellt. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, 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.

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

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung nachfolgender Vorgaben.

(2) Der Auftragnehmer

- ☒ bestellt schriftlich einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Die Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt bzw. sind auf der Webpräsenz des Auftragnehmers leicht zugänglich hinterlegt.
- ☐ ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Er benennt jedoch einen Ansprechpartner und teilt dem Auftraggeber dessen Kontaktdaten mit.
- ☐ hat seinen Sitz außerhalb der Union und benennt einen Vertreter in der Union gem. Art. 27 Abs. 1 DS-GVO. Die Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(3) Der Auftragnehmer 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. 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 belehrt die bei der Durchführung der Arbeiten eingesetzten Personen insbesondere darüber, dass sie Daten nur auf Weisung des Auftraggebers 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.

(4) Der Auftragnehmer setzt alle für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO um und hält sie ein. Verbindliche Maßnahmen werden am Ende dieses Vertrags aufgeführt.

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

(6) Der Auftragnehmer informiert den Auftraggeber 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 Auftragnehmer ermittelt.

(7) 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.

(8) Der Auftragnehmer weist die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber nach.

(9) Der Auftragnehmer unterstützt den Auftraggeber vollumfänglich durch geeignete Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der Betroffenen. Soweit eine betroffene Person sich in Ausübung ihrer Rechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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 Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Auslagerung in Unterauftragsverhältnisse

- ☒ Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Er hat dem Unterauftragsverarbeiter dieselben Regelungen aufzuerlegen, die ihm nach diesem Vertrag auferlegt wurden.

- ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma	Anschrift	Leistung
Klicken Sie hier, um Text einzugeben.	Klicken Sie hier, um Text einzugeben.	Klicken Sie hier, um Text einzugeben.

- ☐ Die Auslagerung auf Unterauftragnehmer
- ☐ Der Wechsel der bestehenden Unterauftragsverhältnisse

ist zulässig, soweit

- a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mit einer Vorlaufzeit von vier Wochen schriftlich oder in Textform anzeigt,
- b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- c) 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.

(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 Auftragnehmers (mind. Textform);

(6) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch von ihm beauftragte Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung, der Vorschriften der DS-GVO und weiterer evtl. einschlägiger datenschutzrechtlicher Vorschriften 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).

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

(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 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 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 nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

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

10. Schutzbedarf

(1) Der Schutzbedarf der Anwendung wird als

☐ normal

☒ hoch *(ergänzende Risikoanalyse auf gesondertem Blatt erforderlich)*

☐ sehr hoch *(ergänzende Risikoanalyse auf gesondertem Blatt erforderlich)*

bewertet.

Begründung:

Der Auftragnehmer hat während der gesamten Dauer der Auftragsverarbeitung die in der **Anlage TOM** zu dieser Vereinbarung festgelegten technischen und organisatorischen Maßnahmen einzuhalten.

11. Außerordentliche Kündigung

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

12. Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder seine Unterauftragsverarbeiter bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DS-GVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

(3) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

13. Sonstiges

- (1) Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragnehmers 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 einer evtl. Leistungsvereinbarung nichts Anderes vereinbart ist, Münster.

14. 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.

Für den Auftraggeber:

Für den Auftragnehmer:

Ort, Datum

Ort, Datum

Anlage Technische und organisatorische Maßnahmen

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

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

	voll erfüllt	teilerfüllt	nicht erfüllt	entfällt	„unterstellt“	Bemerkung
Regelungen zur Passwort-Verwendung	☐	☐	☐	☐	☐	
Regelung zur Mobiltelefonbenutzung	☐	☐	☐	☐	☐	
Beschreibung Netzwerkaufbau/Netzkonzept	☐	☐	☐	☐	☐	
Beschreibung der IT-Arbeitsplätze	☐	☐	☐	☐	☐	
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 - Hardwareeinführung - Softwareeinführung - Hardwarenutzung - Softwarenutzung - Hardwareänderung - Softwareänderung	☐	☐	☐	☐	☐	
Personal						
Regelungen Schulungen - Hard- und Software - Datenschutz & IT-Sicherheit	☐	☐	☐	☐	☐	
Verpflichtung von Beschäftigten nach unterschiedlichen Gesetzen	☐	☐	☐	☐	☐	

	voll erfüllt	teilerfüllt	nicht erfüllt	entfällt	„unterstellt“	Bemerkung
Verpflichtung von Beschäftigten der Unterauftragsverarbeitern/ Externen	☐	☐	☐	☐	☐	
Hard- und Software						
Externe Schnittstellen	☐	☐	☐	☐	☐	
Register für - Software - Hardware - Verfahren - 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.
5	Unterstellt	Externe Vergabe. Einbindung von Unterauftragsverarbeitern. Die Umsetzung der empfohlenen Maßnahmen wurde von dem Beauftragten zugesichert.

Für einzelne Teilbereiche kann der Auftraggeber verantwortlich sein (z.B. der Auftraggeber ist voll oder teilweise für die Rechtevergabe/ Berechtigungskonzept im Fachverfahren zuständig). Dementsprechend ist beim Ausfüllen der Checkliste, diese Verantwortung durch den Auftragnehmer zu prüfen und entsprechend zu kommentieren (wird in Beispielfall durch den Auftragnehmer unterstellt).

Infrastruktur	Beispiele
Verhaltensregelung Pfortendienst und Gebäudesicherung	Die Einrichtung eines Pfortnerdienstes hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Die Arbeitsbedingungen des Pfortners sind für die Aufgabenwahrnehmung geeignet auszugestalten. Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben dem Pfortner 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 aufgrund 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 aufgrund 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 die 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 Mobil- Telefonbenutzung (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-Partner 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 Unterauftragsverarbeitern / 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 Datenspeichern informiert? • Ist sichergestellt, dass PCs nicht unkontrolliert von Wechselmedien gebootet werden können?
Register für - Software - Hardware - 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: • Notfalleitlinie 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?
---	---