Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

-Verantwortlicher-
Unternehmen:
Name:
Straße:
PLZ/ Ort:

- Auftraggeber -

und dem/der

- Auftragsverarbeiter-
Unternehmen: Klaus Lünnemann GmbH
Name: Herr Klaus Lünnemann
Straße: Maybachstraße 23
PLZ/ Ort: 49479 Ibbenbüren

- Auftragnehmer -

schließen zur
Vertragsnummer/ Leistungsvereinbarung (**Hauptvertrag**)

1 _____
2 _____
3 _____
4 _____
5 _____
6 _____
7 _____

nachfolgenden Vertrag über die Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer:

Präambel:

Diese Vereinbarung zur Auftragsverarbeitung (AV) ergänzt jede vertragliche Vereinbarung (einschl. aller zugehörigen bzw. entsprechenden Dokumente wie Leistungsbeschreibungen, SaaS, Anhänge, Anlagen, etc.) zwischen ***der Klaus Lünnemann GmbH*** und dem Kunden oder ***der Klaus Lünnemann GmbH*** und mit dem Kunden verbundene Unternehmen über den Bezug von Leistungen, Produkten oder sonstigen (…jeweils unserem Kunden entsprechend) Leistungen ***der Klaus Lünnemann GmbH***, soweit ***die Klaus Lünnemann GmbH*** personenbezogene Daten im Auftrag des Kunden oder mit dem

Kunden verbundene Unternehmen verarbeitet (**Hauptvertrag**).

Sie gilt für alle mit dem Hauptvertrag in Verbindung stehenden Tätigkeiten, bei denen Beschäftigte ***der Klaus Lünnemann GmbH*** oder ***der Klaus Lünnemann GmbH*** beauftragte Dritte personenbezogene Daten im Auftrag des Kunden verarbeiten. Diese AV beinhaltet in Verbindung mit dem Hauptvertrag die dokumentierten Weisungen für die Verarbeitung personenbezogener Daten, Gegenstand, Dauer, Konkretisierung des Auftragsinhalts, Art und Zweck der Verarbeitung, sowie die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Leistungsbeschreibung

(2) Dauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages. Sollten Leistungen auch noch nach Beendigung des Hauptvertrages erbracht werden, so gelten die Regelungen dieser Vereinbarung auch für diese weitere Leistungserbringung für die gesamte Dauer der tatsächlichen Kooperation fort.

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 in der Leistungsvereinbarung bzw. dem Hauptvertrag **.. . .. …..** konkretisiert.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland wird vorher mit dem Auftraggeber abgestimmt und erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. erfüllt sind. Die Überprüfung der besonderen Voraussetzungen erfolgt seitens des Auftragnehmers.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

☒ Personenstammdaten

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

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☒ Vertragsabrechnungs- und Zahlungsdaten

☒ Planungs- und Steuerungsdaten

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

☒ Bankverbindungsdaten

☒ Bestelldaten

☒ Adressdaten

☒ Lieferadressen

☒ Ansprechpartner zu Lieferadressen

☒ Telefonnummer zu Ansprechpartnern der benannten Lieferadressen

☒ E-Mail-Adresse zu Ansprechpartnern der benannten Lieferadressen

☒ Andere, abweichend von der Lieferadresse vom Auftraggeber für die Durchführung einer Anfrage oder eines Auftrags erforderlichen Kontaktdaten

☒ Orts- oder anderen notwendigen Angaben

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Kunden
☒ Interessenten
☒ Abonnenten
☒ Beschäftigte
☒ Lieferanten
☒ Handelsvertreter
☒ Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. 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 [Einzelheiten in Anlage 1].
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, „Recht auf Vergessenwerden", Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Gemäß den Art. 28 bis 33 DS-GVO gewährleistet der Auftragnehmer hierbei die Einhaltung folgender Vorgaben:

(1) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 Abs. 1 DSGVO bestellt hat und wird diesen gegenüber dem Auftraggeber schriftlich oder in Textform (z.B. E-Mail) benennen.

(2) Der Auftragnehmer bestätigt, dass er bei der Durchführung der Arbeiten nur Beschäftigte einsetzt, die gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
Die bezieht sich insbesondere auf:
   - die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
   - 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.

(4) Der Auftragnehmer sichert die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages zu.

(5) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

6. Unterauftragsverhältnisse

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

(2) Der Auftragnehmer kann Unterauftragnehmer (weitere Auftragsverarbeiter) mit der Verarbeitung personenbezogener Daten im Auftrag des Kunden beauftragen.
Die ***Klaus Lünnemann GmbH*** hat dabei sicherzustellen, dass allen Unterauftragsnehmern, die personenbezogene Daten im Auftrag von im Europäischen Wirtschaftsraum ansässigen Kunden im Wege eines Vertrages oder eines anderen Rechtsinstruments nach dem Recht der EU oder eines EU-Mitgliedstaates verarbeiten, mindestens gleichwertige Datenschutzpflichten, wie die in dieser AV geregelten, auferlegt werden, wobei insbesondere hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen vorzusehen sind.

Folgende Unterauftragsnehmer können durch den Auftragnehmer bei der Verarbeitung von personenbezogenen Daten beauftragt werden:

Unterauftragnehmer	Anschrift/ Land	Leistung

Mindestens zwanzig (20) Kalendertage vor der Beauftragung oder eines Wechsels eines neuen Unterauftragsnehmers hat die ***Klaus Lünnemann GmbH*** seine Kunden entsprechend zu informieren. Der Kunde ist berechtigt, der Beauftragung bzw. dem Einsatz eines neuen Unterauftragnehmers bei der Verarbeitung personenbezogener Daten in seinem Auftrag innerhalb einer Frist von zehn (10) Werktagen zu widersprechen. Der Widerspruch ist an die Mailadresse: ***datenschutz@luennemann.de*** zu richten, wobei der vollständige Name (und andere Daten zur eindeutigen Identifizierung) des Kunden zu nennen sowie auf den entsprechenden Hauptvertrag Bezug zu nehmen und Gründe für den Widerspruch anzugeben sind.
Übt der Kunde sein Widerspruchsrecht aus, so hat die ***Klaus Lünnemann GmbH*** nach freiem Ermessen das Recht:

a) vom Einsatz des beanstandeten Unterauftragsnehmer bei der Verarbeitung personenbezogener Daten im Auftrag des Kunden abzusehen und dies dem Kunden schriftlich zu bestätigen

b) den Kunden zu kontaktieren, um eine einvernehmliche Einigung mit ihm zu suchen, z.B. durch Beseitigung des Grundes für den Widerspruch. Kommt zwischen den Parteien eine Vereinbarung zustande, nimmt der Kunde den Widerspruch zurück.
c) den Hauptvertrag insgesamt oder nur hinsichtlich jener Verarbeitung im Auftrag des Kunden zu kündigen, für welche der beanstandete neue Unterauftragsnehmer beauftragt werden soll.
d) Für jede Übermittlung personenbezogener Daten in ein Land außerhalb der EU, müssen die Voraussetzungen des Art. 44 DSGVO erfüllt sein.

(3) 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.

Unterauftragnehmer	Anschrift/ Land	Leistung

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach 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) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der 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-Folgenabschätzung
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 Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

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

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

10. 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, 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.

11. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

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) Nebenabreden bedürfen der Schriftform.

(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen.
Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Ort	Datum	Ort	Datum
- Auftraggeber -		- Auftragnehmer - vertreten durch	

Anlage – Technisch-organisatorische Maßnahmen

1. **Zugangskontrolle**
   Die Zugangskontrolle wird in der DSGVO mit der Zutrittskontrolle zusammengefasst. Absicherung der Gebäude, Fenster und Türen, Sicherheitsglas, Bruch- und Öffnungsmelder, Videoüberwachungs-Anlagen, Alarmanlagen, Zutrittskontroll-Systeme mit Chipkarten-Leser und Besucher-Dokumentation, Passwortrichtlinien, Zwei-Faktor-Benutzeranmeldung, Firewalls, digitale Zertifikate, Verschlüsselung, Schutz vor Schadsoftware, Bildschirmsperre und aktuelle Nutzerverwaltung

2. **Datenträgerkontrolle**
   Spezielle Räume zur Aufbewahrung, Festlegung der Aufbewahrungsfristen, Datensafes, nur kontrolliertes und dokumentiertes Kopieren, Bestandskontrollen, kontrollierte Vernichtung, ordnungsgemäße Verwaltung von Disketten und Druckausgaben

3. **Speicherkontrolle**
   Regeln und festlegen von Befugnissen, installieren von Zugriffschutzsystemen für zentrale und dezentrale Rechner, Richtlinien für die Dateiorganisation, Anwender-Kennung (Userid), persönliches Passwort, Zwang zum periodischen Passwortwechsel, automatische und manuelle Dunkelschaltung des Bildschirms Entriegelung nur über Passworteingabe, führen von Logdateien, maschinelles Auswerten dieser Logdateien nach bestimmten Kriterien, auswerten von Logdateien und Konsolprotokollen, nutzen der betriebssysteminternen Sicherheitsmechanismen

4. **Benutzerkontrolle**
   | Logindateneingabe/Login credentials | Verschluss der Datenstationen, Verwendung von Benutzerkennungen und Passwörtern, Festlegungen zu Datenübertragungen bei Netzarbeit (Abschottung von anderen Netzen, Begrenzung der Netzverwaltung auf 1 oder 2 Nutzer, Festlegung, welche Daten sollen wie übertragen werden), revisionsfähige Dokumentation der Benutzerprofile, revisionsfähige Protokollierung, Einsatz von Sicherheitssoftware, Einsatz von Verschlüsselungsverfahren, Abweisung unberechtigter Benutzer

5. **Zugriffskontrolle**
   | Berechtigungen für Datenbereiche | Berechtigungskonzept, Verwaltung der Rechte durch Systemadministrator, Regelmäßige Prüfung der Zugriffsberechtigungen, Daten verschlüsselt speichern, Regelung für die Löschung der Daten, Protokollierung von Zugriffen auf Anwendungen

6. **Übertragungskontrolle**
   | Mitlesen von Daten, Überprüfung bzw. Verschlüsselung |Verschlüsselung der Daten Passwortschutz einzelner Dokumente , VPN-Tunnel, Firewall, Virenschutz, Intrusion Detection System (IDS), Content-Filter, SSL-Scanner

7. **Eingabekontrolle**
   | Logging der Zugriffe auf personenbezogene Daten |erweiterte Unterweisungen an diese Personen, Stellenbeschreibung, differenzierte Berechtigungen regeln Benutzerrechte, Auswertung von Logfiles bezüglich “Zugang” und “Zugriff”, Auswertungen der Logfiles, bezüglich Erfassen, Ändern und Löschen der Daten, Einsatz von Anwendungssoftware mit “Rollenkonzepten”, Einsatz von Anwendungssoftware mit “differenzierbaren Rechten”

8. **Transportkontrolle**
   | VPN und Verschlüsselung der Daten | **Übertragung:** nur verschlüsselte Daten übermitteln, Schlüssel periodisch ändern, Übermittlungszeiten variieren **Transport:** feste, verschließbare Metallbehälter, Datenträger als Wertsendung verschicken, keine Kennzeichnung der Behältnisse als Datenträger, bei hausinternem Transport die Versandmappen fest verschließen

9. **Wiederherstellbarkeit**
   | Sicherung der Daten und Verschlüsselung der gesicherten Daten, Redundanz und Wiederherstellbarkeit |Erstellen von Datenbanksicherungen, Verwenden von Hardwarenormen, Aufbewahren von Aufzeichnungen zur Hardware, Aufbewahrungen von Aufzeichnungen zur Software, Bereithalten von Ersatzhardware, Bereitstellen von Training und Dokumentation

10. **Zuverlässigkeit**
    | Monitoring Überwachung der Systeme |

11. **Datenintegrität**
    | Regelmäßige Sicherung der Daten und Datenprüfung |

12. **Auftragskontrolle**
    Dokumentation der Weisungen des Verantwortlichen, vertragliche Regelungen, Kontrolle und Überwachung

13. **Verfügbarkeitskontrolle**
    | Redundanz, Schließfach, Zugangskontrolle, Verschlüsselung |Einstufen der Daten nach Vertraulichkeits-, Integritäts- und Verfügbarkeits-Anforderungen der Stelle, Firewall (eventuell auch direkt auf den einzelnen PCs), Virenschutz, Notfallkonzept, Regelungen zu Routern und Switches, Internetverhaltensregelungen aufstellen, Regelung “E-Mail“ , Backup-Konzept und danach erst geregelte Datensicherungen nach den Bedürfnissen der Stelle

14. **Trennbarkeit**
    | Interne Mandantenfähigkeit, Zweck-Bindungs-Prinzip ist gewahrt, Abspeicherung auf verschiedenen Datenträgern oder mindestens in verschiedenen Verzeichnissen, Trennung von Echtzeit- und Test-System, Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |Zweckbindung im Verfahrensverzeichnis genau formulieren und den Zugriffsberechtigten zur Kenntnis bringen, Unterweisung der Mitarbeiter zu diesem Sachverhalt, regeln Benutzerrechte , regeln Backup dahingehend, dass beim Restore die

Trennung erhalten bleibt, Trennung Produktiv und Testdaten, Trennung von Keys/IDs und Nutzdaten, logische und/oder physikalische Trennung der Datenbestände/Datenbanken, Funktionstrennung (Verantwortung/Ausführung), regeln der Datenübermittlung