Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem/ der

_____

-Schule-
nachstehend Verantwortlicher genannt

und dem

Kommunalem Rechenzentrum
Minden-Ravensberg/Lippe
Bismarckstr. 23
32657 Lemgo

_____

-Auftragsverarbeiter-
nachstehend Auftragnehmer genannt

Inhalt

Präambel 2
1. Gegenstand und Dauer des Auftrags 2
(1) Gegenstand .....
(2) Dauer .....
2. Konkretisierung des Auftragsinhalts 2
(1) Art und Zweck der vorgesehenen Verarbeitung von Daten 2
(2) Art der Daten 3
(3) Kategorien der betroffenen Personen 3
3. Technisch-organisatorische Maßnahmen 3
4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 4
5. Unterauftragsverhältnisse 5
6. Kontrollrechte des Verantwortlichen 5
7. Mitteilung bei Verstößen des Auftragnehmers 6
8. Berichtigung, Einschränkung und Löschung von Daten 6
9. Anfragen betroffener Personen 6
10. Weisungsbefugnis des Verantwortlichen 7
11. Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Vertrags 7
12. Haftung und Schadensersatz 7
13. Außerordentliche Kündigung 8
14. Sonstiges 8

Präambel

Das krz stellt den Schulen mit der Webanwendung „Schüler Online“ ein System zur Anwendung bereit, mit dem die erforderlichen Informationen zwischen Schulen, Schülern/Eltern, und Ausbildungsbetrieben ausgetauscht werden können und ist eine Ergänzung zu den üblichen Schulverwaltungssystemen. Zweck dieser Anwendung ist ein verbessertes Übergangsmanagement vor allem zur Durchführung der Anmeldungen sowie zur Schulpflichtüberwachung. Mit der Anwendung können auch Statistiken erstellt, Beratungen unterstützt und Anträge auf Schülerfahrtkosten aufgenommen werden.

Das krz ist ein Kommunaler Zweckverband, der 1977 gegründet worden ist. In seiner Aufgabe als zuverlässiger IT-Dienstleister für Kommunalverwaltungen und kommunale Einrichtungen betreut das krz über 8.000 IT-Arbeitsplätze im Verbandsgebiet, mit drei Kreisen und 36 Gemeinden und Städten. Als erstes kommunales Rechenzentrum bundesweit liegt eine gültige Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik vor. Es bestehen geeignete technische und organisatorische Maßnahmen, um den Anforderungen der DS-GVO zu entsprechen und den Schutz der Rechte der betroffenen Personen zu gewährleisten.

Die Vereinbarung zur Auftragsverarbeitung konkretisiert die Verpflichtung der beiden Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die in Zusammenhang mit dieser Auftragsverarbeitung bestehen.

1. Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags ergeben sich aus dem geschlossenen Hauptvertrag mit der StädteRegion Aachen, daher endet diese Vereinbarung ohne gesonderte Kündigung, wenn der Hauptvertrag gekündigt wird.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Art der Verarbeitung personenbezogener Daten ergibt sich aus dem Verzeichnis von Verarbeitungstätigkeiten dieses wird vom Auftragsverarbeiter in Web-Anwendung bereitgestellt. Der Zweck der Verarbeitung ist die digitale Übermittlung der Bewerbungen für einen Bildungsgang an den weiterführenden Schulen, sowie der Schulpflichtüberwachung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt.

(2) Art der Daten

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

- ☒ Auszubildende
- ☒ Anmeldungen
- ☒ Erziehungsberechtigte
- ☒ Personendaten
- ☒ Schulbildung
- ☒ Berufsschulpflicht
- ☒ Fahrtkosten

(3) Kategorien der betroffenen Personen

Die Kategorien der durch die Vearbeitung betroffenen Personen umfassen:

- ☒ Schüler/innen
- ☒ Erziehungsberechtigte
- ☒ Betriebe (inkl. 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 Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags (siehe Anlage 1). Soweit die Prüfung/ein Audit des Verantwortlichen 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.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftagnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- **a.** Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- **b.** Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29,32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich der Weisung entsprechend des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer überwacht durch regelmäßige Kontrollen, dass die Verpflichtungen eingehalten werden. Des Weiteren unterrichtet der Auftragnehmer regelmäßig über geltende datenschutzrechtliche Bestimmungen.
- **c.** Der Auftragnehmer verpflichtet sich, die im Rahmen des Auftragsverhältnisses zur Verfügung gestellten oder erarbeiteten Unterlagen und Daten sowie ihm sonst bekannt gewordenen Informationen vertraulich zu behandeln und nur im Rahmen der Tätigkeit für dieses Vertragsverhältnis zu nutzen. Diese Verpflichtung besteht auch nach Ende des Vertragsverhältnisses fort.
- **d.** 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 siehe Anlage 1).
- **e.** Der Verantwortlichen und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- **f.** Die unverzügliche Information des Verantwortlichen über Kontrollhandlung und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungs- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- **g.** Soweit der Verantwortlichen 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.
- **h.** Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person im Hinblick auf Kapitel III DS-GVO gewährleistet wird.
- **i.** Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieser Vereinbarung.

5. 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 Telekommunikationsdienstleistungen, 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 Verantwortlichen, auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Verantwortlichen beauftragen. Er hat dem weiteren Auftragnehmer dieselben Regelungen aufzuerlegen, die dem Auftragnehmer nach diesem Vertrag auferlegt wurden.

Der Verantwortlichen stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO und unter der Gewährleistung eines übereinstimmenden Sicherheitsniveaus zu:

OWL-IT, Kommunaler Zweckverband als Körperschaft des öffentlichen Rechts,
Bismarckstraße 23, 32657 Lemgo.

(3) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den weiteren Auftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine weitere Beauftragung gestattet.

(4) Eine weitere Auslagerung durch den weiteren Auftragnehmer bedarf der ausdrücklichen Zustimmung des Verantwortlichen.

(5) Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Auftragnehmer aufzuerlegen.

6. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche 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 zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Verantwortlichen 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 durch eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. ISO 27001-Zertifizierung auf Basis von IT-Grundschutz) erfolgen.

7. Weitere Pflichten im Falle von Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen 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 Verantwortlichen zu melden
- **c)** die Verpflichtung, den Verantwortlichen 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 Verantwortlichen für dessen Datenschutz-Folgenabschätzung
- **e)** die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. 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 Verantwortlichen 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 Verantwortlichen weiterleiten.

(2) Soweit vom Leistungsumfang umfasst sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragnehmer sicherzustellen.

9. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer informiert den Verantwortlichen und leitet den Antrag der betroffenen Person unverzüglich weiter. Er unterstützt den Verantwortlichen weiterhin bei der Erfüllung seiner Pflichten nach Kapitel III DS-GVO im erforderlichen Umfang. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Verantwortlichen nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

10. Weisungsbefugnis des Verantwortlichen

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen verarbeiten. Der Verantwortlichen entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragnehmers, ist nicht zulässig.

(2) Mündliche Weisungen bestätigt der Verantwortlichen unverzüglich schriftlich (E-Mail ist ausreichend). Diese werden durch den Auftragnehmer dokumentiert.

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

11. Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Vertrags

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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 Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen 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 Verantwortlichen übergeben.

12. Haftung und Schadensersatz

(1) Der Auftragnehmer haftet dem Verantwortlichen für Schäden, die der Auftragnehmer, seine Beschäftigten bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder seine Unterauftragnehmer bei der Erbringung der vertraglichen Leistung schuldhaft verursacht.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der EU-DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, gelten die Reglungen des Art. 28 und 82 EU-DSGVO.

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

13. Außerordentliche Kündigung

Unabhängig von den Regelungen über die oben getroffenen Laufzeiten bzw. die Dauer der Vereinbarung steht dem Verantwortlichen 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 Verantwortlichen nicht ausführen kann oder will oder der Auftragnehmer eine Kontrolle des Verantwortlichen oder der nordrhein-westfälischen Datenschutzbeauftragten vertragswidrig verweigert.

14. Sonstiges

(1) Sollten die Daten des Verantwortlichen beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Verantwortlichen als „Verantwortlichen“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf diese Formerfordernis.

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

(4) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Unwirksame Bestimmungen sind von den Parteien durch wirksame zu ersetzen, die dem gewollten Zweck möglichst nahe kommen. Entsprechendes gilt im Falle einer Vereinbarungslücke.

(5) Gerichtsstand ist, sofern nichts anderes vereinbart, Lemgo.

Im Auftrag

Datum, Unterschrift Verantwortlicher Schule	Datum, Unterschrift Auftragnehmer Kommunales Rechenzentrum Minden-Ravensberg/Lippe

Anlage 1
technische und organisatorische Maßnahmen

Die Anlage beschreibt die technischen und organisatorischen Maßnahmen die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung gem. Art. 24 DS-GVO erfolgt. Diese ergeben sich aus Art. 32 Abs. 1 DS-GVO. Der Auftragnehmer hat nachfolgende Maßnahmen hierzu umgesetzt.

Schutzziele	Maßnahme	Umsetzung der Maßnahme
Vertraulichkeit Art. 32 Abs. 1 lit. b) DS-GVO	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	• Elektronische Zutrittskontrolle • Ausgabe von Besucher-/Mitarbeiterausweisen • Regelungen für Firmenfremde • Maßnahmen zur Objektsicherung • Bildung von Sicherheitszonen, Türsicherung
	Zugangskontrolle Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	• Festlegung befugter Personen • Durchführung von Anwesenheitsaufzeichnungen • Regelungen für Firmenfremde • Verschlüsselte Übertragungswege • Boot-Passwörter
	Zugriffskontrolle Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	• Feste Zuständigkeiten gem. Organisationsverteilung • Funktionstrennung • Umsetzung von Teilzugriffsmöglichkeit auf Datenbestände und Funktionen (Rollen- und Berechtigungskonzepte) • Identifizierung gegenüber dem Datenverarbeitungssystem
	Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	• Mandantentrennung • Richtlinien und Arbeitsanweisungen • Verfahrensdokumentation • Regelungen zur Programmierung • Regeln zur System- und Programmprüfung

Integrität Art. 32 Abs. 1 lit. b) DS-GVO	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	• Dokumentation der Abruf- und Übermittlungsprogramme sowie zu den Stellen, an die eine Übermittlung vorgesehen ist • Verpackungs- und Versandvorschriften • Verschlüsselung • Feststellung zur Übermittlung befugter Personen • Datenträger nur an autorisierte Personen • Regelmäßige Bestandskontrollen • Kontrollierte Vernichtung von Datenträgern • Regelung zur Anfertigung von Kopien • Plausibilitätsprüfung • Maßnahmen zur Verhinderung von unkontrollierten Datenabflüssen
	Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	• Führung von Nachweisen der organisatorisch festgelegten Zuständigkeiten für die Eingabe • Dokumentierendes System zur Bearbeitung von Kunden-Tickets • Protokollierung der Eingaben
Verfügbarkeit und Belastbarkeit Art. 32 Abs. 1 lit. b) DS-GVO	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	• Konzept zur Durchführung von regelmäßigen Datensicherungen • Vergabe von Zugriffsberechtigungen im erforderlichen Umfang • Notstromversorgung und Überspannungsschutzeinrichtung • Notfallkonzept (inkl. Brandschutz) • Regelung zur Aufnahme eines Notfallmanagements

Wiederherstellbarkeit Art. 32 Abs. 1 lit. c) DS-GVO	**Maßnahmen zur raschen Wiederherstellbarkeit** Bei einem unvorhergesehenen Zwischenfall ist dafür zu sorgen, dass die personenbezogenen Daten „rasch" ihrem Zweck entsprechend wieder genutzt werden können.	• Konzept zur Sicherung der Datenbestände (automatisiert) • Rechenzentrumsbetrieb an zwei Standorten • Spiegelung der Daten an zwei Standorten
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung Art. 32 Abs. 1 lit. d) DS-GVO	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	• Sorgfältige Auswahl evtl. weiterer Auftragnehmer • Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Verantwortlichen • Formale Auftragserteilung • Kontrolle der Arbeitsergebnisse
	Datenschutz-Management Zum Schutz personenbezogener Daten ist sicherzustellen, dass eine Datenschutzorganisation etabliert ist und Verantwortlichkeiten festgelegt sind.	• Regelungen zum Datenschutz-Management • Einbindung des Datenschutzbeauftragten • Verzeichnisse von Verarbeitungstätigkeiten • Datenschutz-Folgenabschätzung • Etablierte Prozesse nach DS-GVO • Sensibilisierung und Schulung
Pseudonymisierung und Verschlüsselung Art. 32 Abs. 1 lit. a) DS-GVO	**Pseudonymisierung** Die Gestaltung der Datenverarbeitung hat eine Minimierung von Risiken betroffener Personen zu gewährleisten.	• Keine Durchführung aufgrund von Anforderungen des Fachverfahrens
	Verschlüsselung Zugang zu den personenbezogenen Daten ist ausschließlich dem befugten Personenkreis zu gewähren.	• Angemessene Verschlüsselung nach dem Stand der Technik

Es handelt sich bei den beschriebenen technischen und organisatorischen Maßnahmen um keine abschließende Auflistung. Diese und **weitere** Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der in dieser Anlage beschriebenen Schutzziele. Weiterhin unterliegen die Maßnahmen dem technischen Fortschritt und der Weiterentwicklung. Dabei wird das tatsächliche Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten.