

Vereinbarung zur Auftragsverarbeitung

zwischen

Organisation

Anschrift

PLZ/Ort

- Name, Vorname-

Verantwortlicher -

- nachstehend „**Auftraggeber**“ genannt -

und

DRK Landesschule Baden-Württemberg gGmbH

DRK Lerncampus

Karl Berner Straße 6

72285 Pfalzgrafenweiler

- Auftragsverarbeiter -

- nachstehend auch „**Auftragnehmer**“ genannt -

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

- ☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Bereitstellung der Online-Lernplattform DRK-Lerncampus (Definition der Aufgaben).

1.2. Dauer

Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages. Der Auftraggeber kann diese Vereinbarung sowie den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der

Auftragsverarbeiter eine Weisung des Auftraggeber nicht oder nur teilweise ausführt oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Ein schwerwiegender Verstoß liegt dann vor, wenn der Auftragsverarbeiter die Daten des Verantwortlichen für andere als die nach dieser Vereinbarung bestimmten Zwecke verwendet oder gegen eine wesentliche Pflicht aus dieser Vereinbarung verstößt (bspw. bei einem Datenverlust oder bei einer verschuldeten Möglichkeit der unberechtigten Kenntnisnahme durch Dritte).

Weiter ist der Verantwortliche auch bei Nichtvorliegen der Voraussetzungen gem. Satz 2 und 3 berechtigt, diese Vereinbarung und den Hauptvertrag fristlos zu kündigen, wenn der Auftragsverarbeiter wiederholt gegen diese Vereinbarung verstößt. Voraussetzung hierfür ist, dass der Verantwortliche den Auftragsverarbeiter zuvor auf den Verstoß schriftlich oder in Textform (Fax/E-Mail) hingewiesen hat.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

- ☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Nutzung des DRK-Lerncampus im der ausgewählten Nutzungskategorie Basic, Classic, Silber oder Gold.

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 bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2.2 Art der Daten

- ☒ 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)

2.2. Kategorien betroffener Personen

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

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

3. Technisch-organisatorische Maßnahmen

- 3.1. Der Auftragnehmer hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (Anlage 1). Akzeptiert der Auftraggeber die dokumentierten Maßnahmen werden diese Grundlage des Auftrags. Soweit die Prüfung oder ein Audit Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3.2. Der Auftragnehmer weist mindestens alle zwei Jahre sowie jederzeit auf Anforderung des Kunden schriftlich nach, dass er die technischen und organisatorischen Sicherheitsmaßnahmen gemäß dem Verträge sowie der gesetzlichen Bestimmungen einhält. Der Auftragnehmer ist verpflichtet, den schriftlichen Nachweis so zu erbringen, dass der Auftraggeber, den ihm obliegenden Prüfpflichten nachkommen kann.
- 3.3. 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.
- 3.4. Auf Grund des technischen Fortschritts, sowie der zu erwartenden Entwicklungen in der Gesetzgebung kann sich eine Notwendigkeit der Anpassung der getroffenen technischen und organisatorischen Maßnahmen ergeben. 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 und dem Kunden unverzüglich mitzuteilen. Die erforderlichen Anpassungen der technischen und organisatorischen Maßnahmen an die geänderten gesetzlichen Vorgaben hat der Auftragnehmer unverzüglich umzusetzen.

4. Berichtigung, Einschränkung und Löschung von Daten

- 4.1. 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.
- 4.2. Unmittelbar durch den Auftragnehmer sicherzustellen sind die Betroffenenrechte, insbesondere ein Löschkonzept, das Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers; soweit technisch möglich und rechtlich notwendig.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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 folgender Vorgaben:

- a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Roberto Schmidt, Badstraße 39-41, 70372 Stuttgart bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☒ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

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 entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- b) 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 (Anlage 1).
- c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- d) 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.

- e) 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.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

- 6.1. 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.
- 6.2. Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 2 zu diesem Vertrag angeben.
- 6.3. Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.
- 6.4. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen. Satz 1 und 2 gelten entsprechend für einen Vertreter gemäß Art. 27 DSGVO.
- 6.5. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.
- 6.6. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der

Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

- 6.7. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 7 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden.
- 6.8. 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.

7. Kontrollrechte des Auftraggebers

- 7.1. Der Auftraggeber hat das Recht, in Abstimmung mit dem Auftragnehmer Überprüfungen dieser Vereinbarung 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.
- 7.2. 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.
- 7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch geeignete Maßnahmen erfolgen. Dazu zählen insbesondere:
- 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).
- 7.4.** Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

- 8.1. 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 und
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

9. Weisungsbefugnis des Auftraggebers

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

9.2. 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

10.1. 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.

10.2. 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.

10.3. 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. Vergütung

Die Vergütung des Auftragsverarbeiters ergibt sich aus dem zugrundeliegenden Hauptvertrag. Für die Durchführung von Maßnahmen, die in Art. 28 DS-GVO genannt sind und in diesem Vertrags insbesondere nach den Ziffern 4, 7 und 9 steht dem Auftragnehmer keine Vergütung zu.

12. Haftung, Freistellung, Vertragsstrafe

12.1. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung so-wie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Etwaige Haftungsbegrenzungen der Parteien (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung

13. Sonstiges

13.1. Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

13.2. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind vom Auftragnehmer für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

13.3. Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

13.4. Sollte das Eigentum und/oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

13.5. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

13.6. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1

Technische und organisatorische Maßnahmen (TOM)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung / Liste
Automatisches Zugangskontrollsystem ☒	Empfang / Rezeption / Pförtner
Biometrische Zugangssperren	Besucherbuch / Protokoll der Besucher
Chipkarten / Transpondersysteme ☒	Mitarbeiter- / Besucherausweise
Manuelles Schließsystem	Besucher in Begleitung durch Mitarbeiter ☒
Sicherheitsschlösser	Sorgfalt bei Auswahl des Wachpersonals
Schließsystem mit Codesperre	Sorgfalt bei Auswahl Reinigungsdienste ☒



Absicherung der Gebäudeschächte	
Türen mit Knauf Außenseite	✓
Klingelanlage mit Kamera	✓
Videoüberwachung der Eingänge	

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Login mit biometrischen Daten	Erstellen von Benutzerprofilen
Anti-Viren-Software Server	Zentrale Passwortvergabe
Anti-Virus-Software Clients	Richtlinie „Sicheres Passwort“

Anti-Virus-Software mobile Geräte		Richtlinie „Löschen / Vernichten“
Firewall	☒	Richtlinie „Clean desk“
Intrusion Detection Systeme		Allg. Richtlinie Datenschutz und / oder Sicherheit
Mobile Device Management		Mobile Device Policy
Einsatz VPN bei Remote-Zugriffen	☒	Anleitung „Manuelle Desktopsperre“
Verschlüsselung von Datenträgern		2-Faktor-Authentifizierung ☒
Verschlüsselung Smartphones		
Gehäuseverriegelung		
BIOS Schutz (separates Passwort)		
Sperre externer Schnittstellen (USB)		
Automatische Desktopsperre		
Verschlüsselung von Notebooks / Tablet		

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut) ☒	Einsatz Berechtigungskonzepte ☒
Externer Aktenvernichter (DIN 66399)	Minimale Anzahl an Administratoren ☒
Physische Löschung von Datenträgern ☒	Datenschutztesor
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten ☒	Verwaltung Benutzerrechte durch Administratoren ☒

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung ☒	Steuerung über Berechtigungskonzept ☒
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Festlegung von Datenbankrechten ☒
Mandantenfähigkeit relevanter Anwendungen ☒	Datensätze sind mit Zweckattributen versehen

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt) ☒	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren ☒
Pseudonymisierung im Testsystem ☒	

2. Integrität

2.1. Weitergabekontrolle

Maßnahmen, die 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
E-Mail-Verschlüsselung ☒	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschrufen
Einsatz von VPN ☒	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Protokollierung der Zugriffe und Abrufe ☒	Weitergabe in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen ☒
Bereitstellung über verschlüsselte Verbindungen wie sftp, https ☒	Persönliche Übergabe mit Protokoll
Nutzung von Signaturverfahren	



2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten 	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können 
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) 
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts 
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	Klare Zuständigkeiten für Löschungen 

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Ransomware, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept (ausformuliert) ☒
Feuerlöscher Serverraum ☒	Kontrolle des Sicherungsvorgangs ☒
Serverraumüberwachung Temperatur- und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse ☒
Serverraum klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums ☒
USV ☒	Keine sanitären Anschlüsse im oder oberhalb des Serverraums ☒
Schutzsteckdosenleisten Serverraum	Existenz eines Notfallplans (z. B. BSI IT-Grundschutz 100-4) ☒
Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	Getrennte Partitionen für Betriebssysteme und Daten ☒
RAID System / Festplattenspiegelung ☒	
Videoüberwachung Serverraum	
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Interner / externer Datenschutzbeauftragter siehe oben 
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z. B. Wiki, Intranet ...) 	Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet 
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	Regelmäßige Sensibilisierung der Mitarbeiter: Mindestens jährlich 
Anderweitiges dokumentiertes Sicherheits-Konzept	Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt 

	Die Organisation kommt den Informationspflichten nach ☒
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung ☒	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) ☒
Einsatz von Spamfilter und regelmäßige Aktualisierung ☒	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen ☒
Einsatz von Virens Scanner und regelmäßige Aktualisierung	Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenschutzverletzungen
Intrusion Detection System (IDS)	Dokumentation von Sicherheitsvorfällen und Datenschutzverletzungen z. B. via Ticketsystem ☒

Intrusion Prevention System (IPS)	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenschutzverletzungen 

4.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind 	
Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen 	



4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation 
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) 
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln 
	Schriftliche Weisungen an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis 
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	Regelung zum Einsatz weiterer Subunternehmer
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags 

	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
--	---

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

AV-Data GmbH, Im Schlebert 20, 76187 Karlsruhe

Flessio, Thomas Soo & Dominik Strauss GbR, Sperlingweg 3, 88213 Ravensburg

Ausgefüllt für den AUFTRAGNEHMER durch:

Name Martin Ohder
Funktion Abteilungsleiter
Rufnummer 07261 9717-888
E-Mail m.ohder@drk-ls.de


i.A. Martin Ohder
(Unterschrift)

Vom AUFTRAGGEBER auszufüllen:

Geprüft am _____ durch _____ (Datenschutzbeauftragter).

Es besteht kein Klärungsbedarf mehr. Die Vereinbarung kann wie vorliegend abgeschlossen werden.

Mit der Unterschrift wird bestätigt, dass eine Prüfung mit dem zuvor genannten Ergebnis durch den Datenschutzbeauftragten durchgeführt wurde.

Ort, Datum

(Unterschrift)