Vereinbarung über die Auftragsverarbeitung personenbezogener Daten (Art. 28 DSGVO)

LOGINEO NRW

Zwischen

Name der Organisation
Adresse der Organisation
Vertreten durch (Name Organisationsleiter*in)

als Verantwortlicher

und

Kommunales Rechenzentrum Niederrhein
Der Verbandsvorsteher
Friedrich-Heinrich-Allee 130
47475 Kamp-Lintfort

als Auftragsverarbeiter

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen.

(2) Diese Vereinbarung über die Auftragsverarbeitung personenbezogener Daten gilt für die Webanwendung LOGINEO NRW. Der Gegenstand sowie Art, Umfang und Zweck der Verarbeitung ergeben sich aus Anlage 2 (Einzelheiten der Datenverarbeitung). Sie werden bei Bedarf durch entsprechende Weisungen des Verantwortlichen ergänzt. Ferner werden in der Anlage 2 die Kategorien der personenbezogenen Daten, die der Auftragsverarbeiter im Auftrag für den Verantwortlichen verarbeitet, sowie die Kategorie der betroffenen Personen spezifiziert. Die Spezifikation in der Anlage 2 ist für die Vertragsparteien verbindlich, insbesondere darf der Auftragsverarbeiter die Daten nur zu den in der Anlage 2 genannten Zwecken verarbeiten.

§ 2 Pflichten des Verantwortlichen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche verantwortlich.

(2) Der Verantwortliche erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

(3) Der Verantwortliche hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen sind schriftlich zu erteilen.

(4) Wer die weisungsberechtigten Personen des Verantwortlichen und deren Stellvertreter sind, ergibt sich aus Anlage 1 zu dieser Vereinbarung. Weisungsempfänger beim Auftragsverarbeiter ist die Geschäftsleitung.

(5) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln.

§ 3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der

getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen (§ 2 Abs. 2 und 3). Gegenstand, Art und Zweck der Verarbeitung sowie die Arten der personenbezogenen Daten und Kategorien der betroffenen Personen sind in Anlage 2 festgelegt. Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke.

(2) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaten verstößt, so ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung bis zu einer schriftlichen Bestätigung dieser Weisung durch den Verantwortlichen auszusetzen.

(3) Der Auftragsverarbeiter stellt im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen sicher. Er stellt sicher, dass die verarbeiteten Daten von sonstigen Datenbeständen scharf getrennt werden.

(4) Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme. Die Inspektionen werden durch den Verantwortlichen zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, die jedoch in der Regel mind. 7 Tage beträgt, durchgeführt. Der Auftragsverarbeiter darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

(5) 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

schriftlichen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind.

(6) Die Verarbeitung von personenbezogenen Daten in Privatwohnungen (mobile Tele- oder Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist unter der Voraussetzung gestattet, dass die Maßnahmen nach Art. 32 DSGVO auch in diesem Fall sichergestellt sind. Soweit die personenbezogenen Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Verantwortlichen vorher mit dem Auftragsverarbeiter abzustimmen und vom Auftragsverarbeiter sicherzustellen.

(7) Sollte der Schutz personenbezogener Daten durch Maßnahmen Dritter, z.B. Vollstreckungsmaßnahmen oder durch die Eröffnung eines Insolvenzverfahrens oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen vor Umsetzung dieser Maßnahme zu verständigen. Das Eigentum des Verantwortlichen (z. B. Datenträger, Arbeitskopien, Behältnisse) ist rechtzeitig zu kennzeichnen.

(8) Soweit vom Leistungsumfang erfasst, sind das Recht auf Löschung, Berichtigung, Einschränkung der Verarbeitung, Datenportabilität und Auskunft der Betroffenen nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

(9) An der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DSGVO) wirkt der Auftragsverarbeiter durch Zuleitung der erforderlichen Angaben mit. Der Auftragsverarbeiter führt ein eigenes Verzeichnis gem. Art. 30 Abs. 2 DSGVO.

(10) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.

(11) Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen - nach dessen Wahl - auszuhändigen oder zu löschen bzw. zu vernichten. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Verantwortlichen auszuhändigen. Die Lösch- bzw. Vernichtungspflicht besteht nicht für Datenträger, die schriftlich durch den Verantwortlichen und Auftragsverarbeiter von der Löschung bzw. Vernichtung ausgeschlossen wurden.

§ 4 Unterauftragsverarbeiter

(1) Der Auftragsverarbeiter darf die in Anlage 3 genannten Subunternehmer mit der Verarbeitung von personenbezogenen Daten des Verantwortlichen beauftragen.

(2) Der Auftragsverarbeiter nimmt zur Verarbeitung der Daten die in Anlage 3 genannten Unterauftragsverarbeiter in Anspruch. Eine Änderung der Unterauftragsverhältnisse gilt vom Verantwortlichen als genehmigt, wenn nicht innerhalb einer Frist von 4 Wochen nach Kenntnisnahme ein schriftlicher Einspruch gegenüber dem Auftragsverarbeiter erfolgt.

(3) Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer alle Verpflichtungen, die den Auftragsverarbeiter treffen, entsprechend erfüllt hat und das vertragliche Minimum dieser Vereinbarung gewährleistet ist.

§ 5 Datengeheimnis

(1) Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen das Datengeheimnis gemäß Art. 28 Abs. 3 S. 2 lit. b, 29 und 32 Abs. 4 DSGVO zu wahren. Er stellt sicher, dass alle an der Verarbeitung von personenbezogenen Daten des Verantwortlichen beteiligten Personen einer Geheimhaltungspflicht unterliegen.

(2) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragsverarbeiter stellt sicher, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Auskünfte darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

(4) Der Verantwortliche und der Auftragsverarbeiter informieren sich gegenseitig unverzüglich über Kontrollhandlungen bzw. Maßnahmen durch die/ den jeweiligen Landesdatenschutzbeauftragte/n.

(5) Bei dem Auftragsverarbeiter sind die Beauftragten für Datenschutz & IT-Sicherheit, datenschutz@krzn.de, +49 2842 9070 425 / +49 2842 9070 121 tätig. Ein Wechsel ist dem Verantwortlichen unverzüglich anzuzeigen.

§ 6 Datensicherungsmaßnahmen

(1) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen, insbesondere nach Art. 32 DSGVO.

(2) Die als Anlage 4 beigefügte Aufstellung der technischen und organisatorischen Maßnahmen zum Datenschutz wird für den Auftragsverarbeiter als verbindlich festgelegt.

(3) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(4) Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Er unterrichtet den Verantwortlichen unverzüglich, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Verantwortlichen geändert oder ausdrücklich bestätigt wird.

§ 7 Haftung

(1) Vorbehaltlich der Regelung in § 7 (2) wird die gesetzliche Haftung des Auftragsverarbeiters für Schadensersatz wie folgt beschränkt:

(a) Der Auftragsverarbeiter haftet der Höhe nach begrenzt auf den bei Vertragsschluss typischerweise vorhersehbaren Schaden für die leicht fahrlässige Verletzung wesentlicher Pflichten aus dem Schuldverhältnis (d.h. solcher Vertragspflichten, deren Erfüllung die ordnungsgemäße

Durchführung der Vereinbarung überhaupt erst ermöglicht, deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Verantwortliche regelmäßig vertraut, sog. "Kardinalpflichten");

(b) Der Auftragsverarbeiter haftet nicht für die leicht fahrlässige Verletzung nicht wesentlicher Pflichten aus dem Schuldverhältnis.

(2) Die vorgenannte Haftungsbeschränkung gilt nicht in den Fällen einer zwingenden gesetzlichen Haftung sowie bei Übernahme einer Garantie, Vorsatz oder grober Fahrlässigkeit oder jeder Art schuldhaft verursachter Körperschäden.

§ 8 Sonstiges

(1) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch aßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

§ 9 Vereinbarungsdauer

(1) Die Vereinbarung gilt, solange der Auftragsverarbeiter über die „Kooperationsvereinbarung über den Interimsbetrieb 2019 von LOGINEO NRW" zwischen dem Land NRW, vertreten durch das Ministerium für Schule und Bildung, und dem KRZN mit dem Betrieb von LOGINEO NRW beauftragt ist.

(2) Die Vereinbarung endet ferner, ohne dass es einer gesonderten Kündigung bedarf, sofern der Verantwortliche in dem dafür innerhalb der Anwendung vorgesehenen Verfahren von der Möglichkeit Gebrauch macht, die Nutzung von LOGI EO NRW zu beenden.

§10 Wirksamkeit der Vereinbarung

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

(2) Änderungen der Vereinbarung bedürfen der Schriftform. Dies gilt auch für das Schriftformerfordernis selbst.

(3) Die Vereinbarung tritt mit Unterzeichnung in Kraft.

_____	Kamp-Lintfort
Ort, Datum	Kommunales Rechenzentrum Niederrhein Datenschutz & IT-Sicherheit Im Auftrag
_____	_____
Verantwortlicher	für das KRZN als Auftragsverarbeiter

Anlage 1
zur Vereinbarung über die Auftrags Verarbeitung personenbezogener Daten

Benennung der weisungsberechtigten Personen beim Verantwortlichen

Weisungsberechtigt ist

Name: _____

Anschrift: _____

Abteilung: _____

Telefon: _____

Fax: _____

E-Mail: _____

Stellvertreter ist

Name: _____

Anschrift: _____

Abteilung: _____

Telefon: _____

Fax: _____

E-Mail: _____

Anlage 2
zur Vereinbarung über die Auftragsverarbeitung personenbezogener Daten

Einzelheiten der Datenverarbeitung

1. **Kategorien von Personen**, die von dem vorliegenden Auftrag zur Verarbeitung personenbezogener Daten betroffen sind:

• Lehrkräfte, Personal bei der Organisation
• Lehramtsanwärterinnen und Lehramtsanwärter, Lehrkräfte in Ausbildung
• Schülerinnen und Schüler, Eltern
• Schulpersonal (z. B. kommunales Personal, Schulsozialarbeiter
• sonstige Funktionsträger und Funktionsträgerinnen, Externe (z. B. Mitarbeiter im offenen Ganztag, Ausbilder in Ausbildungsbetrieben, ...)

2. **Kategorien der personenbezogenen Daten**, die von dem vorliegenden Auftrag zur Verarbeitung personenbezogener Daten betroffen sind:

• Personenstammdaten (u.a. Name, primäre Rolle, Gruppenzugehörigkeit, ...)
• Verwaltungsdaten im Rahmen der Aufgabenerfüllung der Organisation/ Schule / des ZfsL (u. a. Kontaktdaten)
• Nutzungsdaten (z. B. freiwillig bereitgestellte Dokumente, Kommunikationsinhalte, Forenbeiträge,
• Betriebsdaten (Logfiles, Cookies)

3. **Umfang, Art und Zweck** des vorliegenden Auftrags zur Verarbeitung personenbezogener Daten:

Im Rahmen der Beauftragung durch den Verantwortlichen erhält der Auftragsverarbeiter Daten von ihm oder dessen Kunden zur Datenverarbeitung.
Nachfolgend sind die Verarbeitungszwecke benannt, die von den Diensten erfasst werden:

• Erfüllung des Bildungs- und Erziehungsauftrags
• Ablegen von Dokumenten aus pädagogischem sowie schul-/ZfsL-verwalterischem Kontext
• elektronische Kommunikation
• Zugang zu Lernmitteln
• Nutzung von und Beteiligung am Support-Netzwerk durch Einstellen von eigenen Forumsbeiträgen zur Unterstützung der Nutzerinnen und Nutzer von LOGINEO NRW
• Eröffnen eines Fehlertickets
• Sicherstellen eines störungsfreien Betriebs, Verwaltung der Basisinformationen der Benutzerinnen und Benutzer, Authentifizierung über Benutzerkennung

Anlage 3
zur Vereinbarung über die Auftragsverarbeitung personenbezogener Daten

Unterauftragnehmer

Unterauftragnehmer (Bezeichnung und Adresse)	Inhalt des Unterauftrags	Unterauftragsdauer
Software-Hersteller Metaventis GmbH Bauhausstraße 7c 99423 Weima	Wartung und Support Weiterentwicklung	ungebrenzt

Der Verbandsvorsteher
Kommunales Rechenzentrum Niederrhein

Friedrich-Heinrich-Allee 130
47475 Kamp-Lintfort

Anlage 4

Technische und organisatorische Maßnahmen (TOM) i.S. Art. 25 Abs. 2 und Art. 32 DSGVO

Kommunales Rechenzentrum Niederrhein (KRZN)

Standort: Kamp-Lintfort

Stand: 01.10.2021

Version: 1.1

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 og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1 Vertraulichkeit gem. Art. 32 Abs. 1 DSGVO

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 (für sensible Bereiche)	☒ Sorgfalt bei Auswahl der 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/Token zur Anmeldung wie auch der Einsatz von CallBack- oder 2-Faktor-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 Benutzerprofil (Betriebssystem)
☐ Login mit Chipkarte- / 2-Faktor	☒ Zentrale Passwortvergabe
☒ Anti-Viren-Software Server	☒ Richtlinie/DV/DA „Passwort-Richtlinie"
☒ Anti-Virus-Software Clients	☒ Richtlinie/DV/DA „Löschen / Vernichten"
☐ Anti-Virus-Software mobile Geräte	☒ Richtlinie/DV/DA „Lokale Datenspeicherung"
☒ Sicherheitsgateways	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Intrusion Detection Systeme	☒ Mobile Device Policy
☒ Mobile Device Management	☒ Richtlinie/DV/DA „Manuelle Bildschirmsperre"
☒ Einsatz VPN bei Remote-Zugriffen	☐
☒ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung Smartphones	☐
☐ Gehäuseverriegelung	☐
☒ BIOS Schutz (separates Passwort)	☐
☒ Sperre externer Schnittstellen (USB)	☐
☒ Automatische Bildschirmsperre	☐
☒ Verschlüsselung von Clients	☐

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
☒ lokale Aktenschredder (Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Externer Aktenvernichter (DIN 32757)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☒ Datentresor / Sicherheitszelle / Lampertz-Zelle
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Verwaltung Benutzerrechte durch zugel. 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-, Test- und Entwicklungsumgebungen	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Datensätze sind mit Zweckattributen versehen

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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 abgesicherten System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

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 Networks (VPNs) eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ 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	☐

Weitere Maßnahmen:

Email-Verschlüsselung möglich, soweit technisch notwendige Maßnahmen beim Empfänger umgesetzt sind (Zertifikatsimport(e)).

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, Sicherheitsgateway, 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
☐	☒ 4-Augen Prinzip

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

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, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

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

☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen	☐

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutz-Management im Einsatz	☒ Interner Datenschutzbeauftragter: *Die Beauftragten für Datenschutz & IT-Sicherheit* *Email: datenschutz@krzn.de* *Tel.: +49 2842 90 70 – 425 / -121*
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffs-möglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z.B. Wiki, Intranet, etc.)	☒ 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 Informationssicherheitsbeauftragter: *Die Beauftragten für Datenschutz & IT-Sicherheit* *Email: datenschutz@krzn.de* *Tel.: +49 2842 90 70 – 425 / -121*
☒ 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 Art. 13 und 14 DSGVO 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 Sicherheitsgateways/ALGs und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzvorfällen (einschl. Meldepflicht ggü. Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☒ ISB in Sicherheitsvorfälle und Datenschutzvorfällen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenschutzvorfällen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenschutzvorfällen

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

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 Widerrufrechts 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 getroffenen Sicherheitsmaßnahmen und deren Dokumentation bei Beauftragung Dritter
☐	☒ 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 i.F. Unterauftragsnehmer
☐	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis

☐	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer
☐	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☒ Regelung i.F. von Einsatz weiterer Unterauftragnehmer
☐	☒ Sicherstellung der Vernichtung von Date nach Beendigung des Auftrags