Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung
zwischen dem/der

.....
- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

LCube – Professional Hosting e.K., Hardenbergstr. 15, 31275 Lehrte
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Als ISO/IEC-27001:2022-zertifizierter Anbieter für Hosting-, Cloud- und IT-Betriebsleistungen verpflichtet sich LCube zu einem hohen Maß an Informationssicherheit und Datenschutz. Die nachfolgende Vereinbarung zur Auftragsverarbeitung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien und wird durch technische und organisatorische Maßnahmen gestützt, die im Rahmen unseres zertifizierten Informationssicherheitsmanagementsystems umgesetzt und regelmäßig überprüft werden.

1. Gegenstand und Dauer des Auftrags
(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus der Kundenummer / Leistungsvereinbarung / SLA / ..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts
(1) Art, Zweck und Umfang der Verarbeitung ergeben sich aus der Leistungsvereinbarung und Anlage 1. Die Verarbeitung kann, soweit vom jeweiligen Leistungsumfang umfasst, insbesondere Bereitstellung, Speicherung, Übertragung, Sicherung, Administration, Monitoring, Fehleranalyse, Wartung, Support, Wiederherstellung und Löschung umfassen. Die Verarbeitung erfolgt grundsätzlich in der EU oder im EWR. Eine Verarbeitung in einem Drittland oder durch eine internationale Organisation ist nur auf dokumentierte Weisung des

Auftraggebers oder im Rahmen eines genehmigten Unterauftragsverhältnisses zulässig und setzt die Einhaltung der Art. 44 ff. DSGVO voraus. Der konkrete Dienst, die Produktregion und der einschlägige Transfermechanismus sind maßgeblich.

(2) Art der Daten
Die Art der verarbeiteten personenbezogenen Daten wird grundsätzlich durch die vom Auftraggeber auf den bereitgestellten Systemen, Diensten und Anwendungen gespeicherten, übertragenen oder verarbeiteten Daten bestimmt.
Je nach Nutzung können insbesondere folgende Kategorien personenbezogener Daten betroffen sein:

- Personenstammdaten
- Kommunikations- und Kontaktdaten
- Vertrags-, Abrechnungs- und Zahlungsdaten
- Benutzerkennungen und Authentisierungsdaten
- Inhalts-, Nutzungs-, Verkehrs- und Protokolldaten
- Mitarbeiter-, Kunden-, Lieferanten- und Interessentendaten
- besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO, soweit diese durch den Auftraggeber verarbeitet werden
- sonstige personenbezogene Daten, die vom Auftraggeber oder dessen Nutzern im Rahmen der jeweiligen Anwendung verarbeitet werden

Der Auftragnehmer hat regelmäßig keine Kenntnis vom konkreten Inhalt der durch den Auftraggeber verarbeiteten Daten und verarbeitet diese ausschließlich im Rahmen der technischen Bereitstellung, Speicherung, Übertragung, Sicherung, Administration, Wartung und Supportleistungen gemäß Leistungsvereinbarung.

(3) Kategorien betroffener Personen
Die Kategorien betroffener Personen ergeben sich aus der konkreten Nutzung der beauftragten Systeme und Dienste durch den Auftraggeber.
Hierzu können insbesondere gehören:

- Kunden und Interessenten
- Beschäftigte und Bewerber
- Nutzer und Websitebesucher
- Lieferanten und Dienstleister
- Mandanten, Patienten oder Mitglieder
- Ansprechpartner des Auftraggebers
- sonstige Personen, deren Daten durch den Auftraggeber verarbeitet werden

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 3].

(3) LCube betreibt für den zertifizierten Geltungsbereich ein ISMS nach ISO/IEC 27001:2022. Die ISO-Zertifizierung ist ein Nachweis des Informationssicherheitsmanagementsystems und keine Zertifizierung nach Art. 42 DSGVO.

(4) Die Maßnahmen dürfen aufgrund technischen Fortschritts und Weiterentwicklung angepasst oder durch gleichwertige Maßnahmen ersetzt werden. Das vereinbarte Schutzniveau darf 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 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) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.

Als Ansprechpartner beim Auftragnehmer wird benannt:

Herr Lars Laehn, +49 5132 92197 0, llaehn@lcube.de

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

c) 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].

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

e) 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.

f) 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.

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

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 darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgelisteten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber innerhalb einer Frist von mindestens 4 Wochen vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch 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) Als Nachweise können insbesondere berücksichtigt werden:
Zertifikate und Auditberichte zum ISMS, insbesondere ISO/IEC 27001:2022;
aktuelle Testate, Prüfberichte oder Berichtsauszüge unabhängiger Stellen;
Sicherheitskonzepte, technische Dokumentationen und Selbstauskünfte;
genehmigte Verhaltensregeln nach Art. 40 DSGVO oder Zertifizierungen nach Art. 42 DSGVO, sofern vorhanden.

(4) Geeignete vorhandene Nachweise sind vorrangig zu berücksichtigen. Zusätzlicher Aufwand für nicht routinemäßige Prüfungen kann nach vorheriger Abstimmung vergütet werden, sofern die Prüfung nicht durch einen vom Auftragnehmer zu vertretenden erheblichen Verstoß veranlasst ist.

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 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 – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

11. Ansprechpartner
Ansprechpartner seitens des Auftragnehmers (Name/Fachabteilung/Telefonnr/E-Mail):
Lars Laehn / 0800-5282348-0 / llaehn@lcube.de

Ansprechpartner seitens des Auftraggebers (Name/Fachabteilung/Telefonnr/E-Mail):

_____

12. Sonstiges

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(2) Bei etwaigen Widersprüchen gehen die Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(3) Es gilt deutsches Recht.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftragnehmer	Auftraggeber

Anlage 1 – Beschreibung der Verarbeitung

Merkmal	Vereinbarung / Auswahl
Gegenstand	**Hosting, Betrieb, Cloud-, Server-, Entwicklungs-, Backup-, Security- und Supportleistungen gemäß Leistungsvereinbarung.**
Dauer	**Laufzeit der Leistungsvereinbarung einschließlich technisch erforderlicher Lösch- und Sicherungszyklen.**
Art und Zweck	**Bereitstellung, Speicherung, Übertragung, Sicherung, Administration, Monitoring, Fehleranalyse, Wartung, Support, Wiederherstellung und Löschung, jeweils nur soweit beauftragt.**

Anlage 2 – Genehmigte Unterauftragnehmer

Unternehmen / Sitz	Leistung	Verarbeitungsort	Hinweis
Infrastruktur- und Rechenzentrumsanbieter			
kyberio GmbH Am Mittelfelde 29 30519 Hannover Deutschland	**Rechenzentrum und Infrastruktur**	**Deutschland**	**ISO/IEC 27001:2022**
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	**Rechenzentrum und Hosting-Infrastruktur**	**Deutschland; ggf. Finnland produktabhängig**	**ISO/IEC 27001:2022.**
Cloud- und SaaS-Anbieter			
Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Irland	**Microsoft 365 und weitere gebuchte Microsoft-Cloud-Dienste**	**EU/EWR sowie produkt- und mandantenabhängig weitere Regionen**	**Microsoft Product Terms und Microsoft Products and Services DPA sind maßgeblich.**
Acronis International GmbH Rheinweg 9 8200 Schaffhausen Schweiz	**Backup- und Security-Dienste**	**Gemäß gebuchter Cloud-Region**	**Internationale Verarbeitungskette produktspezifisch; Transfermechanismus prüfen.**
QualityHosting AG Uferweg 40–42 63571 Gelnhausen Deutschland	**Hosting-, Cloud- und SaaS-Dienste**	**Deutschland bzw. produktabhängig**	**Hosted Exchange Lösungen**
Sonstige Dienstleister			
Greenmark IT GmbH Leinstraße 3 31061 Alfeld (Leine) Deutschland	**Domainregistrierung**	**Deutschland / registrarabhängig**	**Nur gebuchte Domainleistungen.**
eBuero AG Hauptstraße 8	**Telefonzentrale**	**Deutschland**	**Kundenkommunikation**

10827 Berlin Deutschland			
Resello Netherlands B.V. Ceintuurbaan 28 8024 AA Zwolle Niederlande	**Distributor für Microsoft- und Acronis-Produkte**	**Niederlande; produktabhängig**	**Nur gebuchte Produkte; Verarbeitungskette produktspezifisch.**

Hinweis: Produktspezifische weitere Auftragsverarbeiter innerhalb der Verarbeitungsketten von Cloud- und SaaS-Anbietern werden gemäß deren jeweils aktuellen Unterauftragnehmerinformationen offengelegt. Der Auftragnehmer stellt dem Auftraggeber die verfügbaren aktuellen Angaben auf Anforderung beziehungsweise über die vorgesehenen Informationswege bereit.

Anlage 3 – Technisch-organisatorische Maßnahmen

1. Geltungsbereich und Sicherheitsorganisation
Diese Anlage beschreibt die organisatorischen und technischen Grundmaßnahmen von LCube für die Erbringung der beauftragten Hosting-, Cloud-, Server-, Entwicklungs- und Supportleistungen. Welche Maßnahme im Einzelfall greift, hängt von Produkt, Systemarchitektur, Risikoklasse, Kundenkonfiguration und Leistungsumfang ab.
LCube betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001:2022. Der zertifizierte Geltungsbereich umfasst Hosting und Betrieb von Webanwendungen, Webseiten, Shopsystemen und Quellcodeverwaltung, die Bereitstellung und den Betrieb von Cloud-, Root- und Managed-Server-Infrastrukturen sowie die Entwicklung von Webseiten und Webanwendungen. Zertifikat-Register-Nummer und Gültigkeitsdatum entnehmen Sie dem Zertifikat in der Anlage.
Maßnahmen physischer Rechenzentren oder produktspezifischer Cloud-Dienste werden durch die jeweiligen Unterauftragnehmer erbracht. Sie werden nachfolgend ausdrücklich als fremde Infrastrukturmaßnahmen gekennzeichnet und nicht als eigene bauliche Maßnahmen von LCube dargestellt.

2. Governance, ISMS und Risikomanagement
LCube steuert Informationssicherheit und Datenschutz über dokumentierte Verantwortlichkeiten und risikoorientierte Prozesse.

Informationssicherheitsmanagement
Sicherheitsziele, Risiken, Richtlinien, Verantwortlichkeiten und Kontrollen werden im ISMS dokumentiert, bewertet und im Rahmen eines kontinuierlichen Verbesserungsprozesses weiterentwickelt. Änderungen an Systemen und Diensten werden entsprechend ihrer Sicherheitsrelevanz bewertet.

Richtlinien und Verantwortlichkeiten
Es bestehen verbindliche Vorgaben unter anderem für Zugriffsschutz, Passwörter und Authentisierung, Umgang mit Informationen, Änderungen, Sicherheitsvorfälle, Datensicherung, Lieferanten und Notfallvorsorge. Rollen und Zuständigkeiten sind festgelegt.

Personal und Vertraulichkeit
Beschäftigte und sonstige berechtigte Personen werden auf Vertraulichkeit verpflichtet. Sicherheits- und Datenschutzanforderungen werden bei Eintritt, Rollenwechsel und Austritt berücksichtigt. Schulungen und Sensibilisierungen erfolgen risikoorientiert.

Lieferantensteuerung
Unterauftragnehmer werden vor Einsatz unter Berücksichtigung von Leistung, Datenzugriff, Verarbeitungsort, Sicherheitsniveau und Nachweisen bewertet. Datenschutz- und Sicherheitsanforderungen werden vertraglich weitergegeben und regelmäßig überprüft.

3. Vertraulichkeit
Maßnahmen verhindern unbefugten Zutritt, Zugang und Zugriff und unterstützen eine zweckgebundene Mandantentrennung.

Zutrittskontrolle bei LCube
Büro- und Arbeitsbereiche sind gegen unbefugten Zutritt gesichert. Schlüssel und sonstige Zutrittsmittel werden kontrolliert vergeben und bei Verlust, Rollenwechsel oder Austritt entzogen. Besucher erhalten nur kontrollierten Zutritt. Systeme mit Kundendaten werden grundsätzlich in dafür vorgesehenen Rechenzentrums- oder Cloud-Umgebungen betrieben.

Physische Sicherheit der Rechenzentren
Je nach gebuchtem Produkt werden Rechenzentren von kyberio/Hostway, Hetzner oder weiteren freigegebenen Anbietern genutzt. Deren dokumentierte Maßnahmen umfassen abhängig vom Standort unter anderem Perimeterschutz, kontrollierten Zutritt, Besucherregelungen, Videoüberwachung, Alarmierung, Brandfrüherkennung sowie redundante Stromversorgung. Maßgeblich sind die aktuellen Nachweise und der konkrete Leistungsstandort.

Zugangskontrolle
Administrations- und Managementzugänge werden über personengebundene Konten und rollenbezogene Berechtigungen gesteuert. Starke Authentisierungsverfahren und Mehrfaktor-Authentisierung werden für besonders schutzbedürftige oder technisch unterstützte Zugänge eingesetzt. Externe Administrationswege werden durch verschlüsselte Verbindungen, Netzbeschränkungen und gegebenenfalls VPN oder vergleichbare Verfahren geschützt.

Zugriffskontrolle
Berechtigungen werden nach Need-to-know und Least-Privilege vergeben. Administrative Rechte sind auf erforderliche Personen beschränkt. Berechtigungen werden bei Rollenänderung und Austritt angepasst beziehungsweise entzogen und risikoorientiert überprüft. Supportzugriffe erfolgen nur, soweit sie für die vereinbarte Leistung oder Fehlerbehebung erforderlich sind.

Trennungskontrolle
Kundenumgebungen werden je nach Produkt logisch oder physisch getrennt. Hierzu dienen insbesondere Mandanten-, Konto-, Projekt-, Netzwerk-, Verzeichnis-, Datenbank-, Virtualisierungs- oder Containergrenzen. Entwicklungs-, Test- und Produktionsumgebungen werden risikoorientiert getrennt; produktive Daten werden nicht ohne Freigabe und angemessene Schutzmaßnahmen für Tests verwendet.

Pseudonymisierung und Datenminimierung
Pseudonymisierung wird eingesetzt, wenn sie für Zweck und Systemarchitektur geeignet ist oder vom Auftraggeber vorgesehen wird. LCube verarbeitet nur die für Leistung, Betrieb, Sicherheit, Abrechnung und Support erforderlichen Daten. Die fachliche Pseudonymisierung von Anwendungsdaten obliegt dem Auftraggeber, sofern nicht ausdrücklich beauftragt.

4. Integrität und sichere Übertragung
Maßnahmen schützen Daten vor unbefugter Veränderung und sichern die Nachvollziehbarkeit administrativer Eingriffe in angemessenem Umfang.

Übertragungs- und Weitergabekontrolle
Für administrative und kundenbezogene Datenübertragungen werden nach technischer Verfügbarkeit etablierte verschlüsselte Protokolle eingesetzt, beispielsweise TLS/HTTPS, SSH, SFTP oder VPN. Zugangsdaten, Schlüssel und Geheimnisse werden nicht über ungeeignete Kanäle übermittelt. Empfänger und Berechtigungen werden vor Weitergabe geprüft.

Eingabe- und Änderungskontrolle
Administrative Vorgänge, Systemereignisse und sicherheitsrelevante Änderungen werden entsprechend den technischen Möglichkeiten und dem Schutzbedarf protokolliert. Protokolle enthalten typischerweise Zeitbezug, Benutzer- oder Systemkennung und Ereignisart. Zugriff auf Protokolle ist beschränkt; Aufbewahrung und Auswertung richten sich nach System, Risiko, Vertrag und gesetzlichen Anforderungen.

Change- und Konfigurationsmanagement
Änderungen an produktiven Systemen werden geplant, autorisiert, dokumentiert und risikoorientiert getestet. Kritische Änderungen können zusätzliche Freigaben oder ein Vier-Augen-Prinzip erfordern. Konfigurationen und Automatisierungen werden, soweit geeignet, versioniert beziehungsweise nachvollziehbar verwaltet.

Datenträger und Löschung
Datenträger werden geschützt gehandhabt. Ausgemusterte oder defekte Datenträger werden nach einem geeigneten Lösch- oder Vernichtungsverfahren behandelt. Bei Infrastrukturpartnern gelten ergänzend deren dokumentierte Lösch- und Vernichtungsprozesse.

5. Verfügbarkeit und Belastbarkeit
Maßnahmen sollen den vereinbarten Betrieb unterstützen und eine zeitgerechte Wiederherstellung nach physischen oder technischen Zwischenfällen ermöglichen.

Redundanz und Infrastruktur
Redundanz, Hochverfügbarkeit und geografische Verteilung richten sich nach der gebuchten Produkt- und SLA-Stufe. Rechenzentrumsanbieter setzen standortabhängig unterbrechungsfreie Stromversorgung, Netzersatzanlagen, Brandfrüherkennung, Klimatisierung, redundante Netzkomponenten und Überwachung ein.

Datensicherung
Sofern Backup Bestandteil der Leistung ist, werden Sicherungsumfang, Intervall, Aufbewahrung, Speicherort und Wiederherstellungsziel produkt- oder kundenspezifisch festgelegt. Sicherungsdaten werden durch Zugriffsschutz und, soweit vom Produkt unterstützt beziehungsweise vereinbart, Verschlüsselung geschützt. Backup ist bei Root- oder Self-Managed-Leistungen nicht automatisch enthalten.

Wiederherstellung
Wiederherstellungsverfahren und -tests richten sich nach Kritikalität, Leistungsumfang und technisch vereinbarten Zielen. Ergebnisse und erkannte Abweichungen fließen in Verbesserungsmaßnahmen ein. Für Anwendungsfunktion und Datenkonsistenz bleibt eine Mitwirkung des Auftraggebers erforderlich, soweit die Anwendung nicht von LCube verwaltet wird.

Monitoring und Alarmierung
Vereinbarte Systeme und Infrastrukturkomponenten werden automatisiert überwacht. Ereignisse werden nach definierten Schwellen, Zuständigkeiten und Eskalationswegen bearbeitet. Umfang und Reaktionszeiten richten sich nach Leistungsbeschreibung und SLA.

Notfallvorsorge
Für wesentliche Betriebs- und Sicherheitsereignisse bestehen Eskalations-, Kommunikations- und Wiederanlaufregelungen. Notfallverfahren werden risikoorientiert überprüft und geübt. Abhängigkeiten von Infrastruktur- und Cloud-Anbietern werden in der Vorsorge berücksichtigt.

6. Schutz vor Schadsoftware und technischen Angriffen
LCube setzt mehrschichtige Schutzmaßnahmen entsprechend Systemtyp, Bedrohungslage und Leistungsumfang ein.

Netzwerk- und Perimeterschutz
Firewalls, Netzwerksegmentierung, Zugriffsbeschränkungen und DDoS-Schutz werden je nach Plattform durch LCube und/oder den Infrastrukturpartner bereitgestellt. Öffentlich erreichbare Dienste werden auf erforderliche Schnittstellen begrenzt.

Schwachstellen- und Patchmanagement
Sicherheitsinformationen und Schwachstellen werden risikoorientiert bewertet. Von LCube verwaltete Systeme erhalten im vereinbarten Umfang Sicherheitsaktualisierungen. Bei Root-, Self-Managed- oder kundenseitig verwalteten Systemen verbleibt die Patchverantwortung beim Auftraggeber, sofern nicht anders vereinbart.

Malware- und Bedrohungsschutz
Je nach Produkt kommen Schutzmechanismen wie Malware-Schutz, Intrusion Detection/Prevention, Web Application Firewall, E-Mail-Schutz oder verhaltensbasierte Erkennung zum Einsatz. Der konkrete Funktionsumfang ergibt sich aus der Leistungsbeschreibung.

Sichere Entwicklung
Bei Entwicklungsleistungen werden Sicherheitsanforderungen risikoorientiert in Planung, Implementierung, Test und Bereitstellung berücksichtigt. Quellcodezugriffe werden rollenbezogen gesteuert; Versionierung und Reviewverfahren werden entsprechend Projekt und Kritikalität eingesetzt.

7. Incident Response und Datenschutzverletzungen
Sicherheitsereignisse werden strukturiert erkannt, bewertet, eingedämmt und nachbereitet.

Erkennung und Meldung
Monitoring, Protokollierung, Meldestellen und Eskalationswege unterstützen die Erkennung von Anomalien und Sicherheitsvorfällen. Beschäftigte sind zur unverzüglichen internen Meldung verpflichtet.

Bearbeitung

Vorfälle werden nach Kritikalität klassifiziert, dokumentiert und mit Maßnahmen zur Eindämmung, Behebung und Wiederherstellung bearbeitet. Relevante Beweismittel und Protokolle werden angemessen gesichert.

Datenschutzbezug
Bei möglicher Verletzung des Schutzes personenbezogener Daten erfolgt eine Bewertung unter Einbindung der zuständigen Funktionen. Betroffene Auftraggeber werden nach den Regelungen der AVV unverzüglich informiert. Die Entscheidung über Meldungen an Aufsichtsbehörden oder betroffene Personen obliegt grundsätzlich dem Auftraggeber.

Nachbereitung
Ursachen, Wirksamkeit der Reaktion und Verbesserungsmöglichkeiten werden nach relevanten Vorfällen ausgewertet und, soweit erforderlich, in Risiken, Maßnahmen, Richtlinien und Schulungen überführt.

8. Regelmäßige Überprüfung und kontinuierliche Verbesserung
Die Wirksamkeit der Maßnahmen wird im Rahmen des ISMS und ergänzender Kontrollen überprüft.

Risikobewertung
Risiken für Informationswerte, Dienste und Verarbeitungstätigkeiten werden risikoorientiert bewertet. Maßnahmen werden anhand von Schutzbedarf, Bedrohungen, Schwachstellen und vertraglichen Anforderungen ausgewählt.

Kontrollen und Audits
LCube nutzt interne Überprüfungen, Managementbewertungen, Kennzahlen, technische Prüfungen und das externe Zertifizierungsaudit als Elemente des Nachweises und der Verbesserung. Abweichungen werden dokumentiert und nachverfolgt.

Datenschutzmanagement
Verarbeitungstätigkeiten, Lösch- und Aufbewahrungsanforderungen, Betroffenenanfragen und Datenschutzvorfälle werden über definierte Verfahren behandelt. Datenschutz-Folgenabschätzungen werden unterstützt, wenn der Auftraggeber sie für eine beauftragte Verarbeitung benötigt.

Privacy by Design und by Default
Bei eigenen Systemen und Entwicklungsleistungen werden Datenminimierung, Zugriffsschutz, sichere Voreinstellungen, Zweckbindung, Aufbewahrung und Löschbarkeit risikoorientiert berücksichtigt. Bei kundenseitig konfigurierbaren Systemen ist der Auftraggeber für die sachgerechte Konfiguration seiner Fachanwendung verantwortlich.

9. Produktspezifische Verantwortungsabgrenzung

Leistungsmodell	LCube	Auftraggeber
Managed Hosting / Managed Server	Betriebssystem und vereinbarte Plattformkomponenten, Monitoring, Patch- und Backup-Leistungen gemäß Vertrag.	Anwendungs- und Inhaltsdaten, Benutzer- und Fachberechtigungen, soweit nicht beauftragt.
Root-/Self-Managed-Server	Bereitstellung der Infrastruktur und vereinbarte Basisleistungen.	Betriebssystem, Anwendungen, Patches, Firewall-Konfiguration,

		Backups und Benutzerverwaltung, soweit nicht zusätzlich beauftragt.
Shared Hosting	Betrieb der Hosting-Plattform und zentraler Plattformkomponenten.	Website-/Anwendungsinhalte, Benutzerkonten und Anwendungskonfiguration.
Cloud-/VEP-Umgebung	Bereitstellung und Betrieb der gebuchten Cloud-Komponenten entsprechend Leistungsbeschreibung.	Konfiguration und Betrieb kundenseitig verwalteter Instanzen und Anwendungen.
Acronis Backup/Security	Bereitstellung, Mandantenverwaltung und Support im gebuchten Umfang.	Auswahl von Workloads, Sicherungsplänen, Aufbewahrung, Region und Wiederherstellungsanforderungen.

10. Nachweise eingesetzter Infrastrukturpartner

Anbieter	Nachweis / Stand	Ausgewählte dokumentierte Maßnahmen	Abgrenzung
LCube – Professional Hosting e.K.	ISO/IEC 27001:2022, gültig bis 14.08.2028	ISMS für den zertifizierten Hosting-, Cloud-, Server-, Quellcode- und Entwicklungsbereich.	Eigene Organisations- und Betriebsmaßnahmen.
kyberio GmbH / Standort Hannover	Sicherheitskonzept; Re-Zertifizierungsverfahren gesondert nachzuweisen	Mehrzonen-Zutritt, Videoüberwachung, Operation Center, USV/NEA, Brandfrüherkennung, Monitoring und Notfallvorsorge.	Physische und infrastrukturelle Maßnahmen des Rechenzentrums.
Hetzner Online GmbH	ISO/IEC 27001:2022, Zertifikat ZN-2025-35, gültig 27.09.2025–26.09.2028	Zutrittskontrolle, Videoüberwachung, USV/Notstrom, Brandfrüherkennung, redundante Netze und DDoS-Schutz.	Standort- und produktabhängige Infrastrukturmaßnahmen.
Acronis International GmbH	ISO/IEC 27001:2022, Zertifikat IS 689002, Ablauf 02.10.2027	Sicherheit und Verfügbarkeit der Acronis Cyber Cloud und verarbeiteter Daten im zertifizierten Geltungsbereich.	Cloud-Dienst; Region und internationale Verarbeitungskette sind produktspezifisch.

11. Änderungsmanagement dieser Anlage

LCube darf die Maßnahmen an technische Entwicklungen, Risiken und Leistungsänderungen anpassen, sofern das Schutzniveau insgesamt nicht abgesenkt wird. Wesentliche Änderungen

werden dokumentiert und dem Auftraggeber in geeigneter Form zugänglich gemacht.
Produktspezifische Vereinbarungen und Anweisungen gehen dieser allgemeinen Beschreibung vor.

LCUBE PROFESSIONAL HOSTING

ZERTIFIKAT

Die Zertifizierungsagentur
Digitales Institut zur Zertifizierung internationaler Standards

bestätigt, dass

LCUBE PROFESSIONAL HOSTING

LCube - Professional Hosting e.K.
Hardenbergstr. 15
31275 Lehrte
Deutschland

für den Geltungsbereich

Hosting und Betrieb von Webanwendungen, Webseiten, Shopsystemen und Quellcodeverwaltung sowie Bereitstellung und Betrieb von Cloud-, Root- und Managed-Server-Infrastrukturen und Entwicklung von Webseiten und Webanwendungen

ein Informationssicherheitsmanagementsystem nach **ISO 27001:2022** aufgebaut hat. Die normkonforme Umsetzung wurde durch ein Zertifizierungsaudit nach dem **Standard der ISO 27006** bestätigt.

Dieses Zertifikat ist gültig bis 14. August 2028
Zertifikat-Register-Nr. 260814 11 ISMS

Dr. Jens-Uwe Meyer

Dr. Jens-Uwe Meyer, DICIS Vorstand
ISO 27001 Lead Auditor
IRCA Zertifikats Nr. 6211145
Leipzig, den 14.08.2026

Digital Institute for Certification of International Standards DICIS

BvUZ
Mitglied im Bundesverband unabhängiger Zertifizierungsstellen www.bvuz.de

27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022 27001:2022