GenoAkademie
Bildung mit mehrWert.

Anlagen zum Nutzungsvertrag von VR-Bildung

Gültig ab: 01.01.2026

Anlagen

Anlage 1 Gesellschafter, Akademien und Hauptmandanten

Die VR Bildung GbR betreibt ein Bildungsportal (im Folgenden: „Bildungsportal“ genannt). Gesellschafter der VR-Bildung GbR sind derzeit die Regionalakademien der Genossenschaftsverbände und die ADG Akademie Deutscher Genossenschaften e.V.. Die operative Geschäftsführung der VR-Bildung GbR wird aktuell durch die GenoAkademie GmbH & Co. KG ausgeübt.

Gesellschafter:

Firma	Adresse	Kontakt	Registerdaten
GenoAkademie GmbH & Co KG	Raiffeisenstraße 10-16 51503 Rösrath-Forsbach	Telefon: +49 2205 803 9500 E-Mail: ksc@genoakademie.de	Registergericht: Köln Registernummer: HRA 36645 USt.-ID. Nr.: DE 115 668 346 LEI: 52990038E6QPGC9PCT59
ABG GmbH	Leising 16 92339 Beilngries	Telefon: +49 8461.650-1350 E-Mail: info@abg-bayern.de	Registergericht: Ingolstadt Registernummer: HRB Nr.: 6585 USt.-ID. Nr.: DE296117466 LEI: 3912002NQAFT8DXIK840
Genossenschaftsverband Weser-Ems e.V	Raiffeisenstraße 26 26122 Oldenburg	Telefon: +49 441 21003-0 E-Mail: info@gvweser-ems.de	Registergericht: Oldenburg Registernummer: 1709447 USt.-ID. Nr.: DE117472084 LEI: 529900R0MESIPG3HCC80
ADG Akademie Deutscher Genossenschaften e.V.	Schloss Montabaur 56410 Montabaur	Telefon: +49 26 02 14-0 E-Mail: service@adg-campus.de	Registergericht: Montabaur Registernummer: VR684 USt.-ID. Nr.: DE 149338636 LEI 391200QHRKMKMKPWXY82

Akademien:

Firma	Adresse	Kontakt	Registerdaten
GenoAkademie GmbH & Co. KG	Raiffeisenstraße 10-16 51503 Rösrath-Forsbach	Telefon: +492205 803 9500 E-Mail: ksc@genoakademie.de	Registergericht: Köln Registernummer: HRA 36645 USt.-ID. Nr.: DE 115 668 346 LEI: 52990038E6QPGC9PCT59
ABG GmbH	Leising 16 92339 Beilngries	Telefon: +49 8461.650-1350 E-Mail: info@abg-bayern.de	Registergericht: Ingolstadt Registernummer: HRB Nr.: 6585 USt.-ID. Nr.: DE296117466 LEI: 3912002NQAFT8DXIK840
Genossenschaftsverband Weser-Ems e.V.	Raiffeisenstraße 26 26122 Oldenburg	Telefon: +49 441 21003-0 E-Mail: digitalemedien@gvweser-ems.de	Registergericht: Oldenburg Registernummer: USt.-ID. Nr.: DE 117472084 LEI: 529900ROMESIPG3HCC80
ADG Akademie Deutscher Genossenschaften e.V.	Schloss Montabaur 56410 Montabaur	Telefon: +49 26 02 14-0 E-Mail: service@adg-campus.de	Registergericht: Montabaur Registernummer: VR684 USt.-ID. Nr.: DE 149338636 LEI 391200QHRKMKMKPWXY82
Atruvia AG	GAD-Str. 2-6 48163 Münster	E-Mail: training@atruvia.de	Registergericht: Frankfurt am Main Registernummer: 102381 USt.-ID. Nr.: DE 143 582320 LEI: 529900KS43WE8U0JAX73
Verband der Sparda-Banken e.V.	Friedrich-Ebert-Anlage 35-37 60327 Frankfurt am Main	E-Mail: info@sparda-verband.de	Registergericht: Frankfurt am Main Registernummer: VR 5221 Ust.-ID. Nr.: DE114108730

Hauptmandanten:

Firma	Adresse	Kontakt	Registerdaten
Union Investment Privatfonds GmbH	Weißfrauenstraße 7 60311 Frankfurt am Main	Telefon: +49 69 2567-0 E-Mail: e-learning@union-investment.de	Registergericht: Frankfurt am Main Registernummer: HRB 9073 USt.-ID. Nr.: DE114105135 LEI: 529900AVKTTLJSX76Y76
Bausparkasse Schwäbisch Hall AG	Crailsheimer Str. 52 74523 Schwäbisch Hall	Telefon: +49 791 46 4444 E-Mail: sandra.rauscher@schwaebisch-hall.de	Registergericht: Stuttgart Registernummer: HRB 570105 USt.-Id. Nr.: DE 146 782 527 LEI: 529900JZXXU699FCKK89
R+V Allgemeine Versicherung AG	Raiffeissenplatz 1 65189 Wiesbaden	Telefon: +49 611 533-0 E-Mail: vr-bildung@ruv.de	Registergericht: Wiesbaden Registernummer: HRB 2188 USt.-ID. Nr.: DE 8111 983 34 LEI: 529900Z5KBA9KJP6EK09
Reisebank AG	Platz der Republik 6 60325 Frankfurt am Main	Telefon: +49 69 97 88 07 – 650 E-Mail: kundenservice@reisebank.de	Registergericht: Frankfurt am Main Registernummer: HRB 41672 USt.-ID. Nr.: DE 812257728 LEI: 529900CMFR5GQHWTXY51
SCHUFA Holding AG	Kormoranweg 5 65201 Wiesbaden	Telefon: +49 611 – 92780 E-Mail: impressum@schufa.de	Registergericht: Wiesbaden Registernummer: HRB 12286 USt.-ID. Nr.: DE 209 268 827
TeamBank AG	Beuthener Str. 25 90471 Nürnberg	Telefon: +49 911 53 90 – 2000 E-Mail: info@teambank.de	Registergericht: Nürnberg Registernummer: HR B 15409 USt.-ID. Nr.: DE 812 486 546

Firma	Adresse	Kontakt	Registerdaten
			LEI: 529900XIPMQFJ8PTB895
VR-Smart Finanz AG	Hauptstraße 131-137 65760 Eschborn	Telefon: +49 6196 99 5401 E-Mail: ines.limberg@vr-smart-finanz.de	Registergericht: Frankfurt am Main Registernummer: HRB 45 655 USt.-ID. Nr.: DE 114 139978 LEI: 529900MPCPC7QMXEAH49

Anlage 2 Kundengruppen und Kataloge

Die folgende Tabelle zeigt die verschiedenen Kundengruppen in VR-Bildung (siehe Spalte 1) und die jeweils standardmäßig zugeordneten Kataloge (übrige Spalten):

Banken	Regional-akademie*)	ADG	Atruvia	BSH	R+V	SmartFinanz	Teambank	Schufa	Sparda-Verband
Volks- und Raiffeisenbanken	x	x	x	x	X	x	X**)	x	
PSD Banken	x	x	X*****)	X	X	X	X**)	X	
Spardabanken	x	x	X*****)	X	X	X	X**)	X	X
Kirchenbanken	x	x	X	X	X	X	X**)	X	
Privatbanken	X***)		X*****)	Auf Anfrage	Auf Anfrage	Auf Anfrage	Auf Anfrage	X	
Sonstige Banken	X****)		X*****)	Auf Anfrage	Auf Anfrage	Auf Anfrage	Auf Anfrage	x	

*) Regionalakademie des AUFTRAGGEBERS.
**) Nur Partnerbanken der Teambank AG
***) AUFTRAGGEBER der Atruvia AG und Regionalakademie
****) AUFTRAGGEBER der Regionalakademien
*****) Kunden der Atruvia

Sofern der AUFTRAGGEBER auch eine Anzeige der Kataloge weiterer Regionalakademien wünscht, so kann er dies gegenüber der jeweiligen Regionalakademie per E-Mail (gemäß Anlage 6) anzeigen. Die Umsetzung der Anzeige erfolgt über die VR-Bildung GbR.

Je nach vertraglicher Vereinbarung werden die Kataloge im Rahmen der Mandanteneinrichtung und Konfiguration den jeweils berechtigten Kundengruppen (Kunden) zugewiesen. Die Zuweisung erfolgt auf Basis obiger Tabelle.

Den Nutzern (Mitarbeiter der AUFTRAGGEBER) werden die Kataloge wie folgt angezeigt:

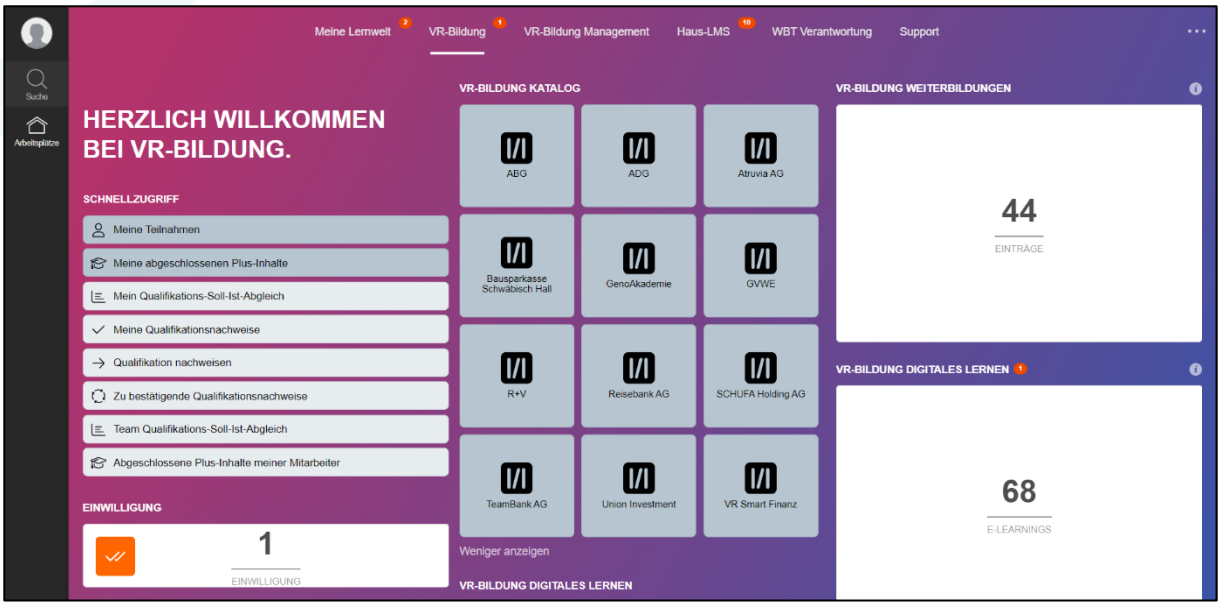

Abbildung 1: Beispielhafte Abbildung für alle Kunden

Kostenfreie Angebote der Akademien und der Hauptmandanten (Contentlieferanten) können

durch die Mitarbeiter der berechtigten AUFTRAGGEBER nach erklärter Einwilligung zu Datenschutzhinweisen direkt über die bereitgestellten Kataloge gebucht oder

durch den Administrator des AUFTRAGGEBERS (Bildungsmanager / Lizenzmanager) einem Nutzer über die Lizenzverwaltung zugewiesen und nach dessen Bestätigung der Einwilligungserklärung (Datenschutzhinweis) geöffnet werden.

Mit der Buchung oder Zuweisung ist lediglich das Recht zum Abspielen des oder der Inhalte verbunden. Anpassung, Änderung und Download der Inhalte ist für alle ausgeschlossen.

Kostenpflichtige Buchungen können derzeit nur direkt über die Akademien und deren Buchungsportale vorgenommen werden.

Contentlieferanten und Akademien sind für ihre auf der Plattform bereitgestellten Bildungsangebote selbst verantwortlich.

Ansprechpartner der Hauptmandanten zu Fragen hinsichtlich des Contents können der Anlage 6 entnommen werden.

Anlage 3 System- und Leistungsbeschreibung

Innerhalb des Bildungsportals (siehe Abbildung 3) unterscheidet die VR-Bildung GbR zwischen Akademien, Inhaltsgebern (nachstehend Contentlieferanten oder Hauptmandanten genannt) und AUFTRAGGEBERN. Die Regionalakademien unterhalten über Nutzungsverträge und den korrespondierenden Auftragsdatenverarbeitungsverträgen die direkte Geschäftsbeziehung mit den AUFTRAGGEBERN zum Bildungsportal. Contentlieferanten und Akademien stellen ihre Bildungsangebote über jeweils eigene Kataloge zur Verfügung, die je nach Berechtigung automatisch den Kundengruppen zugewiesen werden (gemäß Anlage 2).

Akademien und Contentlieferanten werden als eigenständige Mandanten innerhalb des Bildungsportals mit einer klaren und eindeutigen Mandantentrennung geführt (gemäß Abbildung 2).

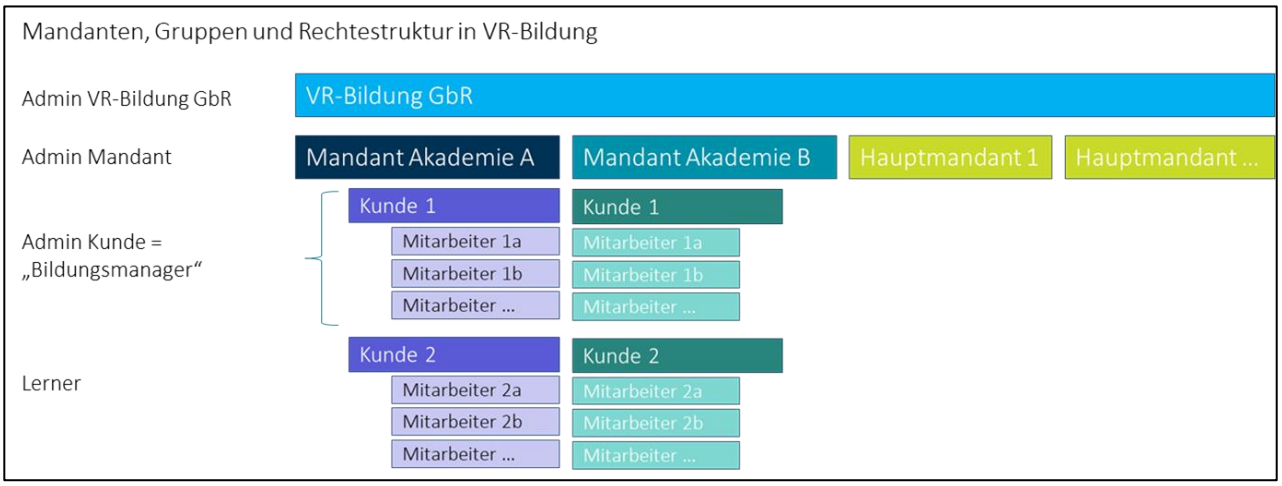

Abbildung 2: Mandanten – Gruppen – Rechte

AUFTRAGGEBER und ihre Mitarbeiter sind im System als eigenständige Gruppe im Mandanten des Vertragspartners zugeordnet. Für alle Instanzen gibt es individuelle Rollen und Rechte.

Die Administratoren (Admin Mandant) der Akademien können hierbei alle dem Mandanten zugewiesene AUFTRAGGEBER, Nutzer, Kurse, Lizenzen (Nutzungsvereinbarungen), Buchungen, Qualifikationen und Historien einsehen und bearbeiten.

Alle Akademien (gemäß Anlage 1) innerhalb des Bildungsverbundes haben Zugriff auf die Nutzer des Bildungsportals, um einen übergreifenden Datenaustausch und eine konsistente Nutzerdatenpflege zu ermöglichen. Hiermit wird eine verzahnte Bildungshistorie, ein redundanzfreier Nutzerdatenbestand und die Dokumentation von Pflichtqualifikationen über alle Akademien hinweg gewährleistet. Die Verzahnung der individuellen Akademiesysteme (Homepage und Seminarmanagementsystem) mit dem Bildungsportal wird nachstehend am Ende der Anlage 3 beschrieben.

Den Hauptmandanten werden keine AUFTRAGGEBER und Nutzer der Akademien zugewiesen, es sei denn, es liegt eine anderslautende Weisung des AUFTRAGGEBERS vor. Sie sind damit vom Nutzerzugriff ausgeschlossen. Ihr Angebot beschränkt sich auf das kostenfreie Angebot von Onlinekursen, welche in einem Katalog dem AUFTRAGGEBER bereitgestellt werden. Zugriffsberechtigungen zu den Katalogen können der Anlage 2 entnommen werden.

Alle Lernelemente und Lernangebote werden über Core 2 ausgespielt (siehe Abbildung 3).

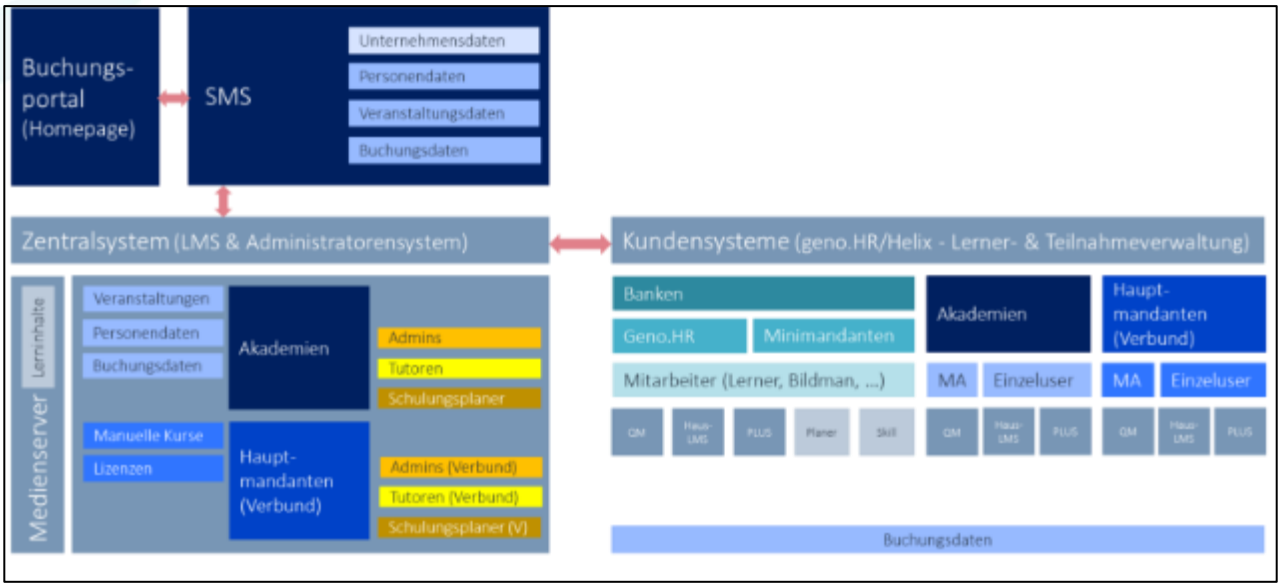

Abbildung 3: Gesamtarchitektur

Die Administratoren des AUFTRAGGEBERS werden im System mit der Rolle “Bildungsmanager” hinterlegt. Die Rechte sind auf die eigene Gruppe beschränkt.

Die Rolle Bildungsmanager wird durch den AUFTRAGGEBER über den geno.HR-Accountadministrator oder durch den AUFTRAGNEHMER über die Benennung des Ansprechpartners in Anlage 6 durch den Dienstleister Perbility vergeben. Die Rolle Bildungsmanager umfasst auch die Nutzerpflege, sofern die Datenversorgung nicht per Schnittstelle (z.B. Entgeltabrechnung der PERRAS GmbH) erfolgt. Darüber hinaus können Bildungsmanager Reportings von den Ihnen zugeordneten Nutzern einsehen. Eine Übersicht der Funktionalitäten kann der Abbildung 4 entnommen werden.

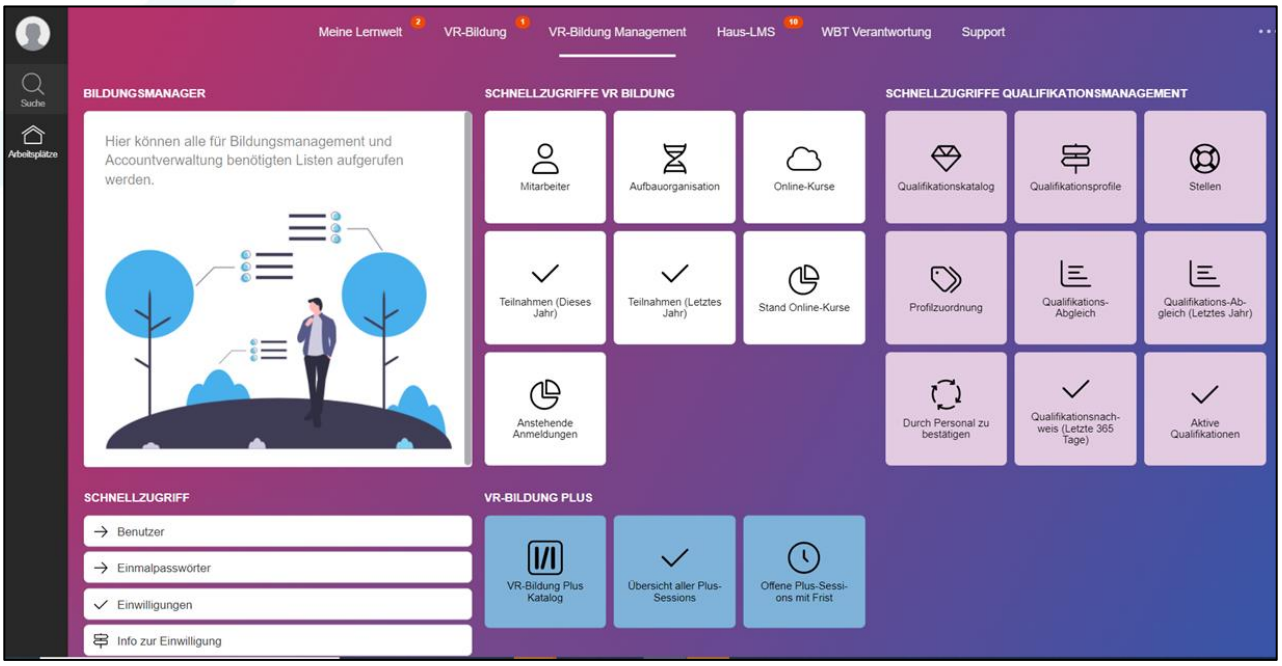

Abbildung 4: Bildungsmanagercockpit im Zentralsystem

Lerner wiederum können ihre eigene Nutzerdaten, Buchungen, Teilnahmen und Lernstände einsehen (siehe Abbildung 5).

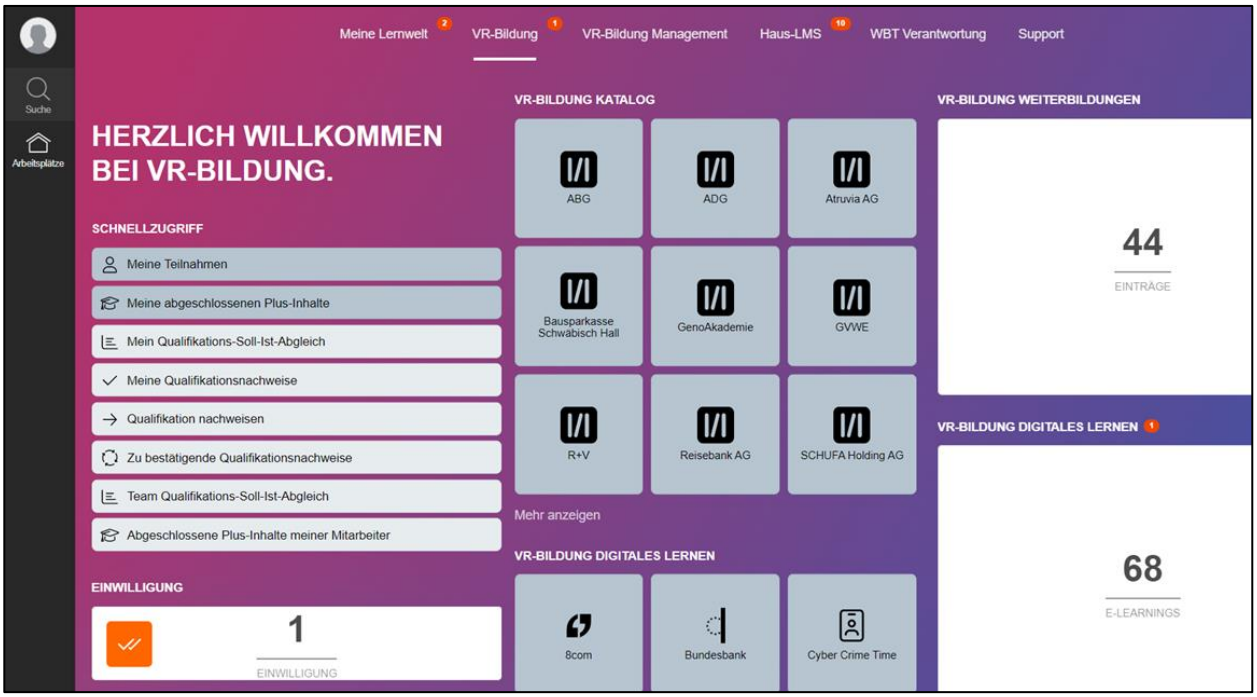

Abbildung 5: Lernercockpit

Hinweis: Die auch sichtbaren Module Qualifikationsmanagement, VR-Bildung PLUS und das Haus-LMS sind kostenpflichtige Erweiterungen zum Hauptvertrag (gemäß 0)

Kunden mit vorhandenen geno.HR-Zugang:

Der Zugang zum Portal wird direkt über den Vertriebsarbeitsplatz (Atruvia) mittels Single-Sign-On oder einem alternativen Zugang für das Lernen zu Hause über eine eigene Domain des angeschlossenen Unternehmens (z.B. https://vrb-kunde.geno.hr.peras.de/) und einer 2 Faktor Authentifizierung ermöglicht.
Nutzerdaten werden sofern vorhanden über eine Schnittstelle der geno.HR-PM Suite der AUFTRAGGEBER direkt mit dem Bildungsportal ausgetauscht. Grundlage dafür ist eine Datenfreigabevereinbarung für alle AUFTRAGGEBER gegenüber der PERAS GmbH.

Auf Basis der Vereinbarung werden nachfolgende Daten ausgetauscht:

- Organisationsdaten, wie Organisationseinheiten, Stellen, Führungszuordnungen, Vertretung – sofern in geno.HR-PM angelegt
- Identifikationsdaten, wie Personalnummer, Geno-User-ID
- Mitarbeiterstammdaten: Vor- und Nachname, Titel, Geburtsdatum, Geburtsname
- Bilddaten, wie Mitarbeiterfoto – sofern in geno.HR-PM angelegt
- Kommunikationsdaten, wie E-Mail, Telefonnummer
- Weiterbildungsdaten, wie Anmeldungen/Teilnahmen an Weiterbildungen, WBT-Lernstände – sofern in geno.HR-PM angelegt oder im Zentralsystem initiierte und genehmigte Bestellungen eines autorisierten Mitarbeiters
- Qualifikationsdaten, wie Qualifikationsnachweise, Qualifikationen – sofern in geno.HR-PM angelegt

Der Zugang für Lerner dieser Kunden erfolgt über Core 1 (siehe Abbildung 4).

Kunden ohne geno.HR-Zugang:

Alle übrigen Bankkunden der Regionalakademien (Privatbanken und deren Beteiligungsunternehmen mit Bankbezug) erhalten, soweit nichts anderes vereinbart wurde, Zugang über ein neu einzurichtendes geno.HR-Kundensystem. Dies setzt eine Datenfreigabeerklärung sowie eine Vertragsbeziehung mit der Peras GmbH voraus, welche den direkten Zugang über den Vertriebsarbeitsplatz (Atruvia) per SSO ermöglicht.

Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Herbeiführung der erforderlichen vertraglichen Vereinbarung.

Ist der AUFTRAGGEBER nicht Kunde der Atruvia AG, so kann kein direkter Zugang über den Vertriebsarbeitsplatz erfolgen. Ein Absprung des Lerners in das Zentralsystem erfolgt über ein eigenes Kundensystem.

Eine Schnittstellenanbindung zum HR-System des AUFTRAGGEBERS kann gegen Entgelt für nachstehende Systeme beauftragt werden (DATEV, P&I Loga, CSS eGECKO, Workday, SAGE, AKDB). Wird keine Schnittstelle beauftragt, so erfolgt die Nutzerverwaltung manuell durch einen verantwortlichen Administrator (Bildungsmanager) des AUFTRAGGEBERS.

Verzahnung der Akademiesysteme mit der Lernplattform VR-Bildung:

Nachstehend können die für den AUFTRAGGEBER relevanten Informationen zu den mit der Bildungsplattform verbundenen Akademiesystemen entnommen werden.

GenoAkademie GmbH & Co. KG (nachstehend GenoAkademie genannt)

Zentrales Buchungsportal der GenoAkademie ist die Homepage mit der Domain www.genoakademie.de. Über die Homepage sind Buchungsberechtigte (gemäß Anlage 6) ermächtigt für Mitarbeiter kostenpflichtige Bildungsangebote verbindlich bei der GenoAkademie zu buchen. Im Backend der Homepage werden die Nutzer / Mitarbeiter mit den Nutzerdaten des Bildungsportals synchronisiert, so dass der Buchungsberechtigte bereits mit der Buchung über die Homepage eine direkte Verknüpfung zum Nutzer vornehmen kann. Mit der direkten Verknüpfung des Nutzers mit der Buchung entsteht ein redundanzfreier Datenfluss beginnend im Buchungsportal.

Die Buchung wird im Anschluss an das Seminarmanagementsystem der GenoAkademie übertragen. Im Seminarmanagementsystem wird die Buchung einer Veranstaltung zugewiesen und verbindlich gegenüber dem AUFTRAGGEBER und dem Nutzer über das Seminarmanagementsystem bestätigt. Das Seminarmanagementsystem synchronisiert ebenfalls die Nutzerdaten mit der Lernplattform.

Nach der Verarbeitung der Buchungsinformationen im Seminarmanagementsystem der GenoAkademie erfolgt die Übergabe der Buchung an das Bildungsportal. Die Buchung erscheint als Teilnahme im Lernercockpit, sowie im Bildungsmanagercockpit des Bildungsportals. Sofern der AUFTRAGGEBER das Modul „Veranstaltungsmanagement" der PERRAS GmbH lizenziert hat, erscheint die Buchung auch in diesem System.

Darüber hinaus findet eine Synchronisation folgender Informationen statt:

- Lernhistorien
- Informationen zu Bildungsmaßnahmen (Qualifikationen, Teilnahmebescheinigungen, Zertifikate)
- Erfüllung von Nachweispflichten gegenüber dem AUFTRAGGEBER / Nutzer (Dies dient der Erfüllung von Nachweispflichten gegenüber dem AUFTRAGGEBER / NUTZER und ermöglicht eine Überwachung der korrekten Datenverarbeitung über die Systeme hinweg.)

Systeme und Dienstleister der GenoAkademie:

System	Subunternehmer	Tätigkeit	Datenverarbeitung	Hosting
Homepage	Digit.ly GmbH, Jordanstraße 26a, 30173 Hannover	Bereitstellung Homepage und Buchungsportal	Deutschland	Deutschland
Seminarmanagementsytem	Genoverband e.V.	Bereitstellung Microsoft dynamics 365 business central als On premise Lösung über Server des Genoverbandes bis 31.12.2025, ab 01.01.2026: Semiro (U2D als On premise Lösung über Server des Genoverbandes e.V.	Deutschland	Deutschland

Zusammenspiel der Systeme der GenoAkademie:

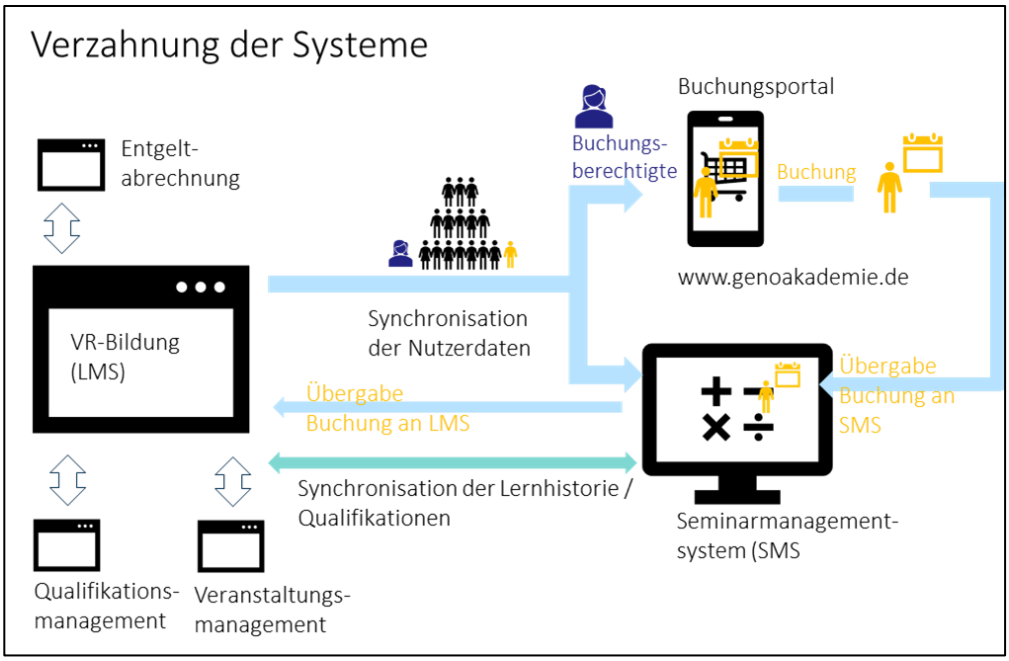

Abbildung 6: Verzahnung mit den Akademiesystemen der GenoAkademie

ABG GmbH

Zentrales Buchungsportal der ABG ist die Homepage mit der Domain www.abg-bayern.de. Über die Homepage sind Buchungsberechtigte (siehe Anlage 6) ermächtigt für Mitarbeiter kostenpflichtige Bildungsangebote verbindlich bei der ABG zu buchen. Im Backend der Homepage werden die Nutzer / Mitarbeiter mit den Nutzerdaten der Lernplattform synchronisiert, so dass der Buchungsberechtigte bereits in der Buchung über die Homepage eine direkte Verknüpfung zum Nutzer vornehmen kann. Mit der direkten Verknüpfung des Nutzers mit der Buchung entsteht ein redundanzfreier Datenfluss beginnend im Buchungsportal.

Die Buchung wird im Anschluss an das Seminarmanagementsystem der ABG übertragen. Im Seminarmanagementsystem wird die Buchung einer Veranstaltung zugewiesen und verbindlich gegenüber dem AUFTRAGGEBER und dem Nutzer über das Seminarmanagementsystem bestätigt. Das Seminarmanagementsystem synchronisiert ebenfalls die Nutzerdaten mit der Lernplattform.

Nach der Verarbeitung der Buchungsinformationen im Seminarmanagementsystem der ABG erfolgt die Übergabe der Buchung an die Lernplattform VR-Bildung. Die Buchung erscheint als Teilnahme im Lernercockpit, sowie im Bildungsmanagercockpit. Sofern der AUFTRAGGEBER das Modul „Veranstaltungsmanagement" der PERAS GmbH lizenziert hat, so erscheint die Buchung auch in diesem System.

Über den Buchungsprozess hinaus besteht eine Synchronisation zu Lernhistorien und mit Bildungsmaßnahmen verknüpften Informationen zu beispielsweise erreichten Qualifikationen zum korrekten Ausweis für Teilnahmebescheinigungen und Zertifikaten, sowie der Erfüllung der grundsätzlichen Nachweisverpflichtung von Teilnahmen der Akademien gegenüber dem AUFTRAGGEBER und dem Nutzer, sowie zur Überwachung der korrekten Datenverarbeitung über die Systeme hinweg.

Systeme und Dienstleister der ABG GmbH:

System	Subunternehmer	Tätigkeit	Datenverarbeitung	Hosting
Homepage	Chamaeleon AG, Robert-Bosch-Straße 12, 56410 Montabaur	Bereitstellung Homepage und Buchungsportal	Deutschland	GVB
Seminar-management-system	x-cellent technologies GmbH, Rosenkavalierplatz 10, 81925 München	Entwicklung	Deutschland	GVB

Genossenschaftsverband Weser-Ems:

Zentrales Buchungsportal der Genossenschaftsakademie ist die Homepage mit der Domain www.gawrastede.de. Über die Homepage sind Buchungsberechtigte (siehe Anlage 6 ermächtigt für Mitarbeiter kostenpflichtige Bildungsangebote verbindlich bei der Genossenschaftsakademie Weser-Ems zu buchen. Im Backend der Homepage werden die Nutzer / Mitarbeiter mit den Nutzerdaten der Lernplattform synchronisiert, so dass der Buchungsberechtigte bereits in der Buchung über die Homepage eine direkte

Verknüpfung zum Nutzer vornehmen kann. Mit der direkten Verknüpfung des Nutzers mit der Buchung entsteht ein redundanzfreier Datenfluss beginnend im Buchungsportal.

Die Buchung wird im Anschluss an das Seminarmanagementsystem der Genossenschaftsakademie Weser-Ems übertragen. Im Seminarmanagementsystem wird die Buchung einer Veranstaltung zugewiesen und verbindlich gegenüber dem Kunden und dem Mitarbeiter (Lerner) über das Seminarmanagementsystem bestätigt. Das Seminarmanagementsystem synchronisiert ebenfalls die Nutzerdaten mit der Lernplattform.

Nach der Verarbeitung der Buchungsinformationen im Seminarmanagementsystem der Genossenschaftsakademie Weser-Ems erfolgt die Übergabe der Buchung an die Lernplattform VR-Bildung. Die Buchung erscheint als Teilnahme im Lernercockpit, sowie im Bildungsmanagercockpit. Sofern der Kunde das Modul „Veranstaltungsmanagement" der PERAS GmbH lizenziert hat, so erscheint die Buchung auch in diesem System.

Über den Buchungsprozess hinaus besteht eine Synchronisation zu Lernhistorien und mit Bildungsmaßnahmen verknüpften Informationen zu beispielsweise erreichten Qualifikationen zum korrekten Ausweis für Teilnahmebescheinigungen und Zertifikaten, sowie der Erfüllung der grundsätzlichen Nachweisverpflichtung von Teilnahmen der Akademie gegenüber dem Kunden und dem Teilnehmer, sowie zur Überwachung der korrekten Datenverarbeitung über die Systeme hinweg.

Systeme und Dienstleister des Genossenschaftsverbandes Weser-Ems:

System	Subunternehmer	Tätigkeit	Datenverarbeitung	Hosting
Homepage	incognito GmbH & Co. KG Robert-Bosch-Straße 19c 48153 Münster	Bereitstellung Homepage und Buchungsportal	Deutschland	Hetzner (ISO 27001) **https://www.hetzner.com/de/unternehmen/zertifizierung/**
Seminar-management-system	Genossenschaftsverband Weser-Ems e.V. (Genossenschaftsakademie)	Bereitstellung Seminarverwaltung HUSAR (Basis Gedys Seminarverwaltung) als on premise Lösung über Server des GVWE.	Deutschland	Server des GVWE

ADG:

Beschreibung:

Die VR-Bildung bietet den genossenschaftlichen Banken über deren Personalmanagement System ein integriertes Lernmanagementsystem an. Alle Akademien aus dem genossenschaftlichen Verbund stellen dort den Banken gemeinsam ihre jeweiligen Bildungsangebote in Katalogen zur Verfügung.

Wenn ein User in VR-Bildung die Veranstaltungen der ADG im Katalog durchsucht, kann er in jeder Detailansicht der jeweiligen Veranstaltung zum Buchungssystem der ADG abspringen. Die dahinter gelagerten Buchungsprozesse werden über ein Shop System (Magento Commerce) an die ERP-Software (MS Dynamics NAV) weitergereicht und dort verarbeitet. Hierüber werden Auftragsbestätigung und weitere Einladungskommunikation an den Kunden zurückgesendet.

Technische Komponenten:

Geno HR	VR-Bildung
Personalmanagement System der genossenschaftlichen Finanzgruppe aus dem Hause Perbility.	Lernmanagementsystem und integrierte Plattform der VR-Bildung Magento Commerce Shopsystem aus dem Hause Adobe Dynamics NAV 2019 / Business Lösung Unitop ERP-System von Microsoft mit der Erweiterung Unitop aus dem Hause GOB als Seminarmanagement System.

Datenübertragung, Datenfluss:

Übertragen des Bildungsangebots (Katalog)

Die ADG stellt über Magento eine REST API zur Verfügung an der VR-Bildung den Katalog der ADG abholen kann. Die Übertragung erfolgt über eine verschlüsselte SSL-Verbindung, die Server der VR-Bildung authentifizieren sich über einen eindeutigen Token.

Es werden alle Veranstaltungen des aktuellen ADG-Angebots bereitgestellt, die Veranstaltungen sind nach Ausführungsformaten (Präsenz, Online), sowie verschiedenen banktypischen Qualifizierungen kategorisiert. Als weitere Merkmale werden Zeitraum, Termine, Preise, Titel, Seminarnummer, Zielgruppe, sowie Beschreibungstexte und Bilder mitgeliefert.

Verarbeitung der Anmeldung

Der Kunde bucht über die Website der ADG (Shopsystem). Hier kann er direkt aus VR-Bildung abspringen, oder über die Homepage der ADG zum Angebot navigieren.

Zur Buchung ist ein persönlicher Login erforderlich.

Zu jeder Buchung sind Anmeldedaten des jeweiligen Teilnehmers erforderlich (Vor- und Nachname, Emailadresse), sowie einige Daten zur Hotel Übernachtung, falls gewünscht.

Diese Daten erhält der Kunde als Zusammenfassung via Email. Diese Daten werden außerdem an das Seminarmanagement System (NAV) weitergereicht. Nach erfolgreicher Prüfung der Anmeldung, erhält der

Kunde eine Auftragsbestätigung, die jeweiligen Teilnehmer eine Einladung zu ihrer Veranstaltung, ggfs. mit weiteren Informationen.

Übertragung der Anmeldeinformationen

Die ADG stellt der VR-Bildung über eine REST API folgende Daten zur Verfügung:

- Buchungsstatus eines Teilnehmers zu der jeweiligen Veranstaltung mit den jeweiligen Terminen, zur Weiterverarbeitung in dem Personalmanagement System
- Teilnahme Status des jeweiligen Teilnehmers zu den Veranstaltungen (Teilgenommen, storniert) zur weiteren Verwendung in dem Personalmanagement System.

Die Übertragung der Daten erfolgt verschlüsselt und das Abholen der Daten erfordert eine Token Authentifizierung der Serververbindung.

Atruvia:

Die Anlage der Trainingsangebote erfolgt im SAP Veranstaltungsmanagement. Die Trainingsangebote werden per Batch an Perbility übertragen und somit in Geno.HR bereitgestellt. Perspektivisch wird hierbei zukünftig auch der Durchführungsstatus übertragen.

Zentrales Buchungsportal für Atruvia AG ist der Atruvia Shop im Atruvia Hub. Nach Auswahl eines Trainingsangebotes in geno.HR kann der User über einen Direktlink den entsprechenden Artikel im Shop aufrufen und die Buchung durchführen.

Systeme und Dienstleister der Atruvia:

System	Subunternehmer	Tätigkeit	Datenverarbeitung	Hosting
Seminarmanagement-system	SAP	Bereitstellung Veranstaltungsmanagement SAP VM	Deutschland	Atruvia AG
Atruvia Shop	SAP	Bereitstellung Shop-Lösung Atruvia Shop	Niederlande	SAP SE

Verband der Sparda-Banken e.V.

Die Anlage der Trainingsangebote erfolgt im GenoLive Veranstaltungsmanagement. Die Trainingsangebote werden manuell in das Zentralsystem übertragen und somit in Geno.HR bereitgestellt.
Das Buchungsportal für die Bildungsangebote des Verbands der Sparda-Banken e.V. ist über die Domain https://sparda-verband.de/spardaakademie/ erreichbar. Nach Auswahl eines Trainingsangebotes im Buchungsportal erfolgt die Übermittlung an den Verband der Sparda-Banken e.V.. Die Teilnehmer werden durch den Verband der Sparda-Banken e.V. im Anschluss manuell im Zentralsystem eingebucht.

Systeme und Dienstleister des Verbands der Sparda-Banken e.V.:

System	Subunternehmer	Tätigkeit	Datenverarbeitung	Hosting
Seminarmanagementsystem	Conventex Gesellschaft für Softwareentwicklung mbH	Anlage von Trainingsangeboten Verwaltung von Trainingsangeboten Buchungsportal	Deutschland	Deutschland

Anlage 4 Zusatzmodule und Erweiterungen

Der Funktionsumfang des Bildungsportals kann durch Zusatzmodule erweitert werden. Für die Aktivierung und Nutzung sowie deren Nutzungsbedingungen dieser Zusatzmodule muss pro Zusatzmodul ein gesonderter Nutzungsvertrag abgeschlossen werden.

Im Folgenden wird der Funktionsumfang der Zusatzmodule beschrieben.

Qualifikationsmanagement:

Das Qualifikationsmanagement erlaubt das effiziente Verwalten und Managen von regulatorisch vorgeschriebenen Mitarbeiterqualifikationen. Gesetzlich vorgeschriebene Anforderungen (Qualifikationen) z. B. nach IDD, WpHGMaAnzV, WKR usw. sind in einem zentralen Qualifikationskatalog gesammelt und können zu Qualifikationsprofilen gebündelt werden. Diese Qualifikationsprofile werden dann den einzelnen Mitarbeitern, Planstellen oder Stellen zugeordnet.

Der Qualifikationskatalog kann auch mit individuellen Qualifikationen erweitert werden. Die Leistungsangebote der Akademien im Bildungsverbund unterstützen jedoch nur die zentral vorgegebenen Qualifikationen.

Der Nachweis der Qualifikationen erfolgt automatisiert aus den Teilnahmen an Bildungsmaßnahmen der in Anlage 1 genannten Unternehmen aus dem Bildungsportal heraus oder manuell durch die Lerner oder die Bildungsmanager (gemäß **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**) über die Funktion „Qualifikationsnachweis“.

Ein automatisierter Soll-Ist-Abgleich, sowie ein stichtagsbezogener Abgleich sind jederzeit möglich.

Haus-LMS:

Das Haus-LMS ermöglicht die Erstellung und Administration von eigenen Online-Kursen im Unternehmen für Mitarbeiter des Unternehmens.

Im Einzelnen bietet das Modul „Haus-LMS“ folgende aufgelistete Möglichkeiten der Nutzung:

- Unbegrenzt, selbst erstellte Inhalte in das “Haus-LMS” hochladen und den eigenen Mitarbeitern zur Verfügung zu stellen.
- E-Learning Kataloge mit eigenen Inhalten aufbauen (z.B. WBTs, Videos, Podcasts, Dokumente, Texte, Links und Aufgaben) oder erworbene Inhalte von anderen Anbietern in den digitalen Bildungskatalog aufzunehmen, sofern die Inhalte des Drittanbieters durch diesen geteilt bzw. bereitgestellt werden.
- Digitale Kurse mit Kurslogiken (Verknüpfen von Inhalten in Abhängigkeit zueinander) erstellen.

- Digitale Lerninhalte mit Präsenzveranstaltungen zu Blended-Learning Szenarien mit Kurslogiken verschmelzen (Hinweis: Nutzung erfordert Vereinbarung zum Veranstaltungsmanagement mit der PERAS GmbH).
- Selbsterstellte Kurse mit einer Qualifikation verbinden (Hinweis: Nutzung erfordert Vereinbarung zum Qualifikationsmanagement mit dem Vertragspartner (Regionalakademie).

VR-Bildung Plus:

VR-Bildung Plus ist eine vertragliche Erweiterung zum Nutzungsvertrag VR-Bildung, die es den AUFTRAGGEBERN ermöglicht vergünstigt Inhalte von Bildungsanbietern außerhalb der genossenschaftlichen Finanzgruppe zu erwerben, im Bildungsportal abzurufen und zu administrieren.

Die Inhalte können darüber hinaus im Modul „Haus-LMS“ verwendet werden.

Die Nutzungsbedingungen der verfügbaren Angebote werden in gesonderten Nutzungsverträgen definiert.

Anlage 5 Service Level Agreement (SLA)

Präambel:

Das Bildungsportal VR-Bildung wird von der VR-Bildung GbR betrieben. Zentraler Dienstleister für die VR-Bildung GbR ist die Firma Perbility GmbH in Bamberg.

Neben den Betriebsleistungen werden, für die in Anlage 3 und Anlage 4 beschriebenen Systeme auch Support- und Unterstützungsleistungen erbracht.

Vertragsgegenstand:

Die Leistungsscheine beschreiben die Leistungen, die im Rahmen des Hostings und des Betriebs des Bildungsportal, sowie den Support für das Bildungsportal erbracht werden.

Rahmenbedingungen für den Betrieb

RZ-Standards

Das LMS wird in einem Rechenzentrum betrieben. Das Rechenzentrum entspricht dem aktuellen Stand der Technik und den gesetzlichen Anforderungen zum Betrieb von sicherheitsrelevanten Datenverarbeitungsanwendungen unter Einhaltung der Bestimmungen der DSGVO und des BDSG.

Service Level

In den Leistungsscheinen sind für bestimmte IT-Leistungen Service Level vereinbart (Service Level Agreements) und bestimmten Leistungsstufen zugeordnet (Sollwerte). Näheres regeln die Leistungsscheine (Anlage 5a Leistungsschein Betrieb; Anlage 5b Leistungsschein Support).

Virenschutz

Sollten die Vertragspartner trotz allseitiger üblicherweise ausreichender Schutzmaßnahmen von Computer-Viren betroffen sein, so trägt jeder Partner seinen aus einem Virenbefall resultierenden Schaden selbst.

Mitwirkungspflichten der VR-Bildung GbR und des AUFTRAGGEBERS

Die VR-Bildung GbR und der AUFTRAGEBER werden die im Folgenden aufgeführten Beistellungen und Mitwirkungspflichten über die Dauer des Vertrages für den Betreiber vollständig, richtig, rechtzeitig und kostenfrei erbringen.

Die VR-Bildung GbR wird beim AUFTRAGGEBER auftretende Mängel oder Störungen schriftlich (per E-Mail) und/oder telefonisch unverzüglich mitteilen. Der AUFTRAGGEBER hat diese Mitteilungspflicht gegenüber der VR-Bildung GbR. Im Übrigen gelten die Mitwirkungspflichten nach den Leistungsscheinen.

Koordination der Zusammenarbeit

Die Mitarbeiter des AUFTRAGGEBERS können sich direkt an den Support des AUFTRAGNEHMER (RegionalAkademien) unter folgenden Supportadressen oder Telefonnummern wenden:

Akademie	Anschrift	Supportmail	Hotline
ABG GmbH	Leising 16 92339 Beilingries	Vr-bildung@abg-bayern.de	keine
GenoAkademie GmbH & Co. KG	Raiffeisenstr. 10-16 51503 Rösrath-Forsbach	*Lms-support@genoakademie.de*	02205-803-9500
Genossenschaftsverband Weser-Ems e.V.	Raiffeisenstr. 26 26122 Oldenburg	digitalemedien@gvweser-ems.de	0441-210-030

Hinweis:

Sofern es sich um fachliche Fragen zu Inhalten aus Onlinekursen der Hauptmandanten handelt, so können Sie sich auch direkt an die in Anlage 6 benannten Ansprechpartner wenden.

Anlage 5a Leistungsschein Betrieb

Gegenstand des Leistungsscheins

Der vorliegende Leistungsschein beschreibt die Leistungen, die im Rahmen des Betriebs des Bildungsportals erbracht werden.

Service Level

Betriebszeiten

Folgende Betriebszeiten werden für die Systeme vereinbart:

Leistung	Wochentag	Uhrzeit
Bedienter Betrieb	Mo-Do*	08:00-17:00
	Fr	08:00-16:00
Unbedienter Betrieb	Übrige Zeit	Übrige Zeit

* ausschließlich der gesetzlichen Feiertage im jeweiligen Bundesland des AUFTRAGNEHMERS, sowie gegebenenfalls auf der jeweiligen Homepage des AUFTRAGNEHMERS kommunizierte Schließzeiten (z.B. Weihnachten bis Neujahr).

Bedienter Betrieb:

Während des bedienten Betriebes werden die Systeme durch den AUFTRAGNEHMER in Verbindung mit dessen Dienstleistern überwacht. Störungen werden ausschließlich in der bedienten Betriebszeit behoben. Es gelten die vereinbarten Service Level.

Unbedienter Betrieb:

Die Systeme sind i. d. R. verfügbar. Es stehen keine Ansprechpartner des Supports zur Verfügung. Problemmeldungen werden mit Beginn des bedienten Betriebes aufgenommen. Es gelten keine Service Level.

Ausfall- und Fehlerbehebungszeiten

Ausfallzeit:

Die Ausfallzeit ist die Zeit, die das Bildungsportal, gemessen am Leistungsübergabepunkt, kontinuierlich nicht zur Verfügung steht.

Fehlerbehebungszeit:

Die Fehlerbehebungszeit ist der Zeitraum zwischen der Meldung einer Störung durch den VERTRAGSNEHMER an den Dienstleister und dem Abschluss der Störungsbeseitigung, d.h. der Wiederherstellung der uneingeschränkten Funktionsfähigkeit der gestörten Leistung.

Berechnungsgrundlage sind die Zeitstempel im Problem-Management-Tool. Der Betreiber strebt folgende Fehlerbehebungszeiten für das Produktionssystem an:

Fehlerklasse	Fehlerbehebungszeit
Systemstillstand, ein Weiterarbeiten jeglicher Art ist nicht mehr möglich.	Max. 24 Std.

Sofern die Störungsmeldung außerhalb der bedienten Betriebszeit erfolgt, beginnt die Fehlerbehebungszeit mit dem Beginn des nächsten bedienten Betriebsfensters.

Sind auftretende Fehler ursächlich auf die Anwendungssoftware bzw. deren Support zurückzuführen, liegen sie nicht in der Verantwortung des Dienstleisters / VR-Bildung GbR.

Verfügbarkeit

Leistung	Service Level
Bedienter Betrieb	Verfügbarkeit / Monat für die Produktionsumgebung

Die gewährleistete Mindestverfügbarkeit des Produktivsystems während des bedienten Betriebes beträgt im Monatsmittel mindestens 96%, bezogen auf die Zeit des bedienten Betriebs eines Kalendermonats.

Messmethode

Die Verfügbarkeit (V) im Monatsmittel berechnet sich für einen Kalendermonat (M) nachfolgender Formel:

$$\frac{Verfügbarkeit}{Monat\ (in\ \%)} = \frac{\frac{Tatsächliche\ Betriebssystemzeit}{Monat + Entschuldbar\ Ausfallzeit}}{\frac{Planmäßige\ Stunden}{Monat}} \times 100$$

Die tatsächliche Betriebssystemzeit bezeichnet die monatliche Gesamtstundenzahl der planmäßigen Stunden des bedienten Betriebes (IST), während das Produktivsystem am Übergabepunkt (Providergateway) zur Verfügung steht.

Die entschuldbare Ausfallzeit steht für diejenige Gesamtzahl der Stunden des bedienten Betriebes innerhalb eines Monats, für die ein Systemausfall in Abstimmung zwischen VR-Bildung GbR und Betreiber geplant wurde.

Planmäßige Stunden stehen für die maximale Verfügbarkeit in Tagen pro Woche und Stunden pro Tag des bedienten Betriebes (SOLL).

Folgende Ausfallzeiten werden in die Berechnung der Verfügbarkeit des bedienten Betriebes nicht mit einbezogen:

- Störungen, die durch den Provider der Datenleitungen verursacht werden und nicht durch den Betreiber kompensiert werden können.
- Störungen, die durch einen Fehler in der Anwendungssoftware des Bildungsportals verursacht werden.
- Störungen, die durch das Unternehmen verursacht wurden
- Zeiten für gemeinsam abgestimmte und geplante Wartungen während der Wartungsfenster, sowie andere gemeinsam mit VR-Bildung GbR geplante Einschränkungen der Verfügbarkeit (z.B. Brandschutzübungen, Security Update, projektbedingte Unterbrechungen).

Anlage 5b Leistungsschein Support

Gegenstand des Leistungsscheins

Der vorliegende Leistungsschein beschreibt die Leistungen, die im Rahmen des Supports des Bildungsportals inkl. LMS seitens des Vertragspartners in Zusammenarbeit mit der VR-Bildung GbR erbracht werden.

Umfang Support

Der Vertragspartner ist zuständig für einen Service Desk für Fehlermeldungen und sonstige Anfragen, sowie die Administration des Bildungsportals.

Service Level

Supportzeiten

Folgende Supportzeiten werden für die Systeme vereinbart:

Leistung	Wochentag	Uhrzeit
Service Desk	Mo-Do*	08:00-17:00
	Fr	08:00-16:00
LMS-Administration	Mo-Do*	08:00-16:00
	Fr	08:00-16:00

* ausschließlich der gesetzlichen Feiertage im jeweiligen Bundesland des Vertragspartners, sowie gegebenenfalls auf der jeweiligen Homepage des Vertragspartners kommunizierte Schließzeiten (z.B. Weihnachten bis Neujahr).

Die Systeme sind i. d. R. verfügbar. Außerhalb der Service Desk Zeiten stehen keine Ansprechpartner des Supports und der LMS Administration zur Verfügung. Problemmeldungen werden mit Beginn der Supportzeiten aufgenommen. Außerhalb der Service Desk Zeiten gelten keine Service Level in Bezug auf Reaktionszeiten.

Reaktions- und Fehlerbehebungszeiten

Reaktionszeit:

Die Reaktionszeit ist der Zeitraum zwischen der Entgegennahme der Incidentmeldung (innerhalb der Supportzeit) durch den Vertragspartner und der Einleitung der Incidentbeseitigung.

Fehlerbehebungszeit:

Die Fehlerbehebungszeit ist der Zeitraum zwischen der Meldung eines Incidents und dem Abschluss der Incidentbeseitigung, d.h. der Wiederherstellung der uneingeschränkten Funktionsfähigkeit der gestörten Leistung.

Der Vertragspartner gewährleistet folgende Reaktionszeiten und strebt folgende Fehlerbehebungszeiten in Zusammenarbeit mit der VR Bildung GbR für das Produktionssystem an:

Fehlerklasse	Reaktionszeit	Fehlerbehebungszeit
Systemstillstand, ein Weiterarbeiten jeglicher Art ist nicht mehr möglich	24 Std.	48 Std.

Sofern die Incidentmeldung außerhalb der Supportzeiten erfolgt, beginnt die Fehlerbehebungszeit mit dem Beginn des nächsten Supportfensters.

Anlage 6 Ansprechpartner

Ansprechpartner der Regionalakademien:

Kategorie	ABG GmbH	GenoAkademie GmbH & Co. KG	Genossenschaftsverband Weser-Ems e.V
Vertragsfragen	vrbildung@abg-bayern.de	Dawid Kazmierowski Telefon: +49 511 9574-5577 E-Mail: dienstleistungen@genoakademie.de	Dr. Gerhard Kroon Telefon: +49 441 21003-660 E-Mail: gerhard.kroon@gvweser-ems.de Josefine Solling Telefon: +49 4402 9382-45 E-Mail: josefine.solling@gvweser-ems.de
Supportfragen	vrbildung@abg-bayern.de	Telefon: +49 2205 803 - 9500 E-Mail: Lms-support@genoakademie.de	Christian Ritter Telefon: +49 4402 9382-43 E-Mail: christian.ritter@gvweser-ems.de Olaf Brunner Telefon: +49 4402 9382-47 E-Mail: olaf.brunner@gvweser-ems.de
Informationssicherheit (ISB)	-	Jan Reinhardt Informationssicherheit@genoakademie.de	-
Datenschutz (DSB)	Frank Lammersen flammersen@gv-bayern.de +49 (89) 2868-3160	Patrick Te-Strote Datenschutz@genoakademie.de	Gvwe-datenschutzbeauftragter@gvweser-ems.de

Weisungsempfänger (siehe Auftragsdatenverarbeitungsvertrag)	Daniel Gronloh sowie seine internen Vertretungen	Eppo Franke Stefan Diehm Benjamin Hetterich	Christian Ritter Olaf Brunner

Ansprechpartner der weiteren Akademien und Hauptmandanten:

Partner	Ansprechpartner	Kontakt
ADG Akademie Deutscher Genossenschaften e.V.	Support	Telefon: +49 26 02 14-0 E-Mail: service@adg-campus.de
Atruvia AG	Support	Telefon: +49 721 4004-0 E-Mail: postfach@atruvia.de
Bausparkasse Schwäbisch Hall AG	Support	Telefon: +49 791 46 4444 E-Mail: sandra.rauscher@schwaebisch-hall.de
R+V Allgemeine Versicherung AG	Support	Telefon: +49 611 533-0 E-Mail: vr-bildung@ruv.de
Reisebank AG	Support	Telefon: +49 69 97 88 07 – 650 E-Mail: kundenservice@reisebank.de
SCHUFA Holding AG	Support	Telefon: +49 611 – 92780 E-Mail: impressum@schufa.de
TeamBank AG	Support	Telefon: +49 911 53 90 – 2000 E-Mail: info@teambank.de
Union Investment GmbH	Support	Telefon: +49 69 2567-0 E-Mail: e-learning@union-investment.de
Verband der Sparda-Banken e.V.	Support	Telefon: +49 6979 2094 540 E-Mail: akademie@sparda-verband.de
VR-Smart Finanz AG	Support	Telefon: +49 6196 99 5401 E-Mail: ines.limberg@vr-smart-finanz.de

Ansprechpartner des AUFTRAGGEBERS:

Ansprechpartner	Name	Vorname	Kontakt
Bildungsmanager[1)]			
Bildungsmanager[1)]			
Bildungsmanager[1)]			
Weisungsberechtigter [2)] (nur eintragen, wenn abweichend von Bildungsmanager/n)			
Weisungsberechtigter [2)] (nur eintragen, wenn abweichend von Bildungsmanager/n)			
Vertragsfragen [3)] (nur eintragen, wenn abweichend von Bildungsmanager/n)			
Vertragsfragen [3)] (nur eintragen, wenn abweichend von Bildungsmanager/n)			
Unternehmenslizenzen [4)] (nur eintragen, wenn abweichend von Bildungsmanager/n)			
Unternehmenslizenzen [4)] (nur eintragen, wenn abweichend von Bildungsmanager/n)			
Accountadministrator [5)]			
Informationssicherheitsbeauftragter [6)]			
Datenschutzbeauftragter [7)]			
Buchungsberechtigte [8)]			
Buchungsberechtigte [8)]			
Buchungsberechtigte [8)]			

1) Bildungsmanager sind Nutzer mit Adminrechten in der Lernplattform. Die Rolle umfasst unter anderem Rechte wie: Nutzerpflege, Verwaltung, Einschreibungen von Nutzern und die Auswertung von Lernergebnissen. Sofern der AUFTRAGGEBER über keinen geno.HR-PM Zugang verfügt, benötigt der AUFTRAGNEHMER einen initial genannten Mitarbeiter, der das Recht zur Vererbung des Rechts an weitere Nutzer erhält. Wenn oben nicht anders angegeben erhalten die Bildungsmanager auch die Informationen zu Vertragsfragen, Vertragsänderungen und Unternehmenslizenzen. Personelle Veränderungen dieser Rolle müssen dem AUFTRAGNEHMER nicht mitgeteilt werden, da die mit der Rolle versehenen Personen für den AUFTRAGNEHMER im System ersichtlich sind.

2) Weisungsberechtige Person: Ausschließlich weisungsberechtigte Personen können dem AUFTRAGNEHMER Aufträge zur Verarbeitung personenbezogener Daten geben.

3) Vertragliche Änderungen nebst Anlagenänderungen werden direkt dem angegebenen Mitarbeiter per E-Mail angezeigt.

4) Vertragliche Anpassungen von Nutzungsvereinbarungen zu Onlinekursen / Web-based Trainings (WBTs) werden direkt per E-Mail oder schriftlich dem relevanten Ansprechpartner angezeigt. Dies können beispielsweise Aktualisierungen von Inhalten oder Bearbeitungsinformationen sein.

5) Accountadministratoren (geno.HR-PM-Kunden) haben das Recht weitere Adminrechte (Bildungsmanagerrechte) für die Lernplattform einzuräumen oder zu entziehen. Incidents oder Rollenanpassungen würden direkt an die Zielgruppe kommuniziert.

6) Der Informationssicherheitsbeauftragte (ISB) erhält alle Informationen, Meldungen und Fragen zur Informationssicherheit.
7) Der Datenschutzbeauftragte (DSB) erhält alle Informationen, Meldungen und Fragen zum Datenschutz.
8) Buchungsberechtigte Personen erhalten Zugriff auf das oder die Buchungsportale der Akademien. In der Regel ist dies die zentrale Homepage der Akademie, über die eine kostenpflichtige Buchung für Nutzer getätigt werden können.

Werden keine Personen für die verschiedenen Rollen angegeben so erfolgt die Kommunikation an die in VR-Bildung hinterlegten Bildungsmanager und die Kompetenzen gemäß den obenstehenden Rollen werden dem/den Bildungsmanager/n eingeräumt.

Ergeben sich Änderungen bei Personen, die nicht die Rolle Bildungsmanager innehaben, so sind diese in Schriftform oder per E-Mail dem AUFTRAGNEHMER mitzuteilen (siehe Ansprechpartner AUFTRAGNEHMER).

Anlage 7 Dienstleister und Subunternehmer

Subunternehmer	Adresse	Tätigkeit	Datenverarbeitung	Hosting
Genoverband – e.V.	Genoverband e.V. Wilhelm-Haas-Platz 63263 Neu-Isenburg Telefon 069 6978-0 E-Mail kontakt@genossenschaftsverband.de	Bereitstellung IT-Infrastruktur und Telekommunikationsservices, Personalverwaltung, und Buchhaltung für die GenoAkademie GmbH & Co. KG und der VR Bildung GbR	Deutschland	Hauseigene Server-Infrastruktur (Wilhelm-Haas-Platz, 63263 Neu-Isenburg)
Perbility GmbH	Perbility GmbH Starkenfeldstraße 21 96050 Bamberg	Hosting, Bereitstellung Personalmanagementplattform	Deutschland	Noris network AG, Thomas-Mann-Straße 16-20, 90471 Nürnberg
Peras GmbH	Peras GmbH Dieselstraße 5 76227 Karlsruhe	Betrieb geno.HR und geno.PM, Datenübertragung in Plattform Personalwesen	Deutschland	Atruvia AG, Fiduciastraße 20, 76227 Karlsruhe
GenoAkademie GmbH & Co. KG	GenoAkademie GmbH & Co. KG Raiffeisenstraße 10-16 51503 Forsbach	Operative Geschäftsführung der VR-Bildung GbR und Administration der Plattform VR-Bildung	siehe Genoverband e.V.	siehe Genoverband e.V.
VR-Bildung GbR	GenoAkademie GmbH & Co. KG Raiffeisenstraße 10-16 51503 Forsbach	Betrieb der Lernplattform VR-Bildung über die operative Geschäftsführung der GenoAkademie GmbH & Co. KG	siehe Genoverband e.V.	siehe Dienstleister der GbR (Perbility GmbH) und Genoverband e.V.

Die VR-Bildung GbR wird betrieben durch deren Gesellschafter (gemäß Anlage 1). Im Rahmen dessen wird das Bildungsportal kontinuierlich weiterentwickelt und der sichere Betrieb gewährleistet.

Die GenoAkademie GmbH & Co. KG wurde per Gesellschaftervertrag der VR-Bildung GbR mit der operativen Geschäftsführung beauftragt. Diese bezieht ihre IT-Dienstleistungen von deren Hauptgesellschafter dem Genoverband e.V..

Der Informationssicherheitsbeauftragte (ISB) und Datenschutzbeauftragter (DSB) des Genoverbandes stellen durch regelmäßige Prüfungen die IT-Sicherheit und die Einhaltung der DSGVO sicher.

Darüber hinaus unterzieht sich der Genoverband, sowie deren Tochtergesellschaften und Beteiligungsunternehmen wie die GenoAkademie GmbH & Co. KG regelmäßig einem ISO 27001 konformen Audit.

Weiterhin unterliegt die VR-Bildung GbR, sowie die GenoAkademie GmbH & Co. KG regelmäßigen Prüfungen der Innenrevision des Genoverbandes e.V.

Neben dem Genoverband e.V. verfügt der Dienstleister Perbility GmbH ebenfalls über eine entsprechende Zertifizierung.

Anlage 8 Informationssicherheit

Geltungsbereich der Anforderungen:

Die im Folgenden beschriebenen Anforderungen beziehen sich ausschließlich auf die von Seiten des AUFTRAGNEHMERS in Verbindung mit der VR-Bildung GbR zu erbringenden vertraglichen Leistungen gemäß der Leistungsbeschreibung des Hauptvertrags VR-Bildung. Die Anforderungen an die Informationssicherheit betreffen somit alle Mitarbeiter, IT-Systeme und Einrichtungen des AUFTRAGNEHMERS, sowie der VR-Bildung GbR, die in eine Verarbeitung der Informationen des AUFTRAGGEBERS involviert sind.

Gewährleistung eines angemessenen Informationssicherheitsmanagements:

Der AUFTRAGNEHMER ist verpflichtet, die zum Schutz der Informationen und Daten des AUFTRAGGEBERS notwendigen technischen und organisatorischen Maßnahmen auch bei der Leistungserbringung durch Dritte sicherzustellen.

Dabei sind die verzahnten Systeme gemäß Anlage 3 zu betrachten und das im Folgenden beschriebene Schutzniveau zu gewährleisten, das vom AUFTRAGNEHMER und der VR-Bildung GbR sicherzustellen sind. Die Systemverantwortung kann nachstehender Abbildung 1 entnommen werden.

Systeme	VR-Bildung GbR	AUFTRAGNEHMER (Regionalakademie)	Sonstige Akademien
Buchungsportal (Homepage)		X	X
Seminarmanagementsystem		X	X
Zentralsystem Bildungsportal	X		
Administration und Weiterentwicklung des Learning Management Systems	X		

Eintrittswahrscheinlichkeit und die potenzielle Schadenshöhe des Risikos aus einem Informationssicherheitsvorfall, sowie der Stand der Technik, gängige Marktstandards (z. B. „IT-Grundschutz-Kompendium – in der aktuellsten Version“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der internationale Sicherheitsstandard ISO/IEC 2700X der International Organisation for Standardization) sind hierbei zu berücksichtigen. Mindestens hat sich der AUFTRAGNEHMER bei der Festlegung geeigneter technischer und organisatorischer Maßnahmen an den Sicherheitsstandards ISO/IEC 27001 (incl. dessen Annex) zu orientieren. In jedem Fall ist auf die Umsetzung der vom AUFTRAGGEBER im Anhang definierten Sollschutzmaßnahmen hinzuwirken.

Über wesentliche Abweichungen, die ein Risiko für die Informationssicherheit darstellen, wird der AUFTRAGNEHMER den AUFTRAGGEBER ohne schuldhaftes Verzögern informieren.

Der AUFTRAGNEHMER wird die technischen und organisatorischen Maßnahmen entsprechend dem technischen Fortschritt und des Bekanntwerdens neuer Risiken für die Informationssicherheit stetig weiterentwickeln. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen, die Einfluss auf die Integrität, Vertraulichkeit, Authentizität oder Verfügbarkeit, der von ihm zu erbringenden Leistungen

haben können, wird der AUFTRAGNEHMER dem AUFTRAGGEBER mitteilen, wobei der AUFTRAGGEBER solchen Änderungen nur aus wichtigem Grund widersprechen kann. Als wichtiger Grund gilt insbesondere, wenn begründeter Anlass zu Zweifeln bezüglich des ordnungsgemäßen Schutzes der Informationen des AUFTRAGGEBERS besteht. Der AUFTRAGGEBER kann jederzeit eine aktuelle Beschreibung der vom AUFTRAGNEHMER konkret getroffenen technischen und organisatorischen Maßnahmen anfordern.

Kontrollrechte des AUFTRAGGEBERS:

Der AUFTRAGNEHMER wird dem AUFTRAGGEBER mindestens einmal jährlich durch geeignete Nachweise belegen, dass er geeignete technische und organisatorische Maßnahmen implementiert hat, um ein dem Risiko für die Informationssicherheit angemessenes Schutzniveau zu gewährleisten. Falls die von dem AUFTRAGNEHMER vorgelegten Nachweise nicht geeignet sind, dieses zu belegen oder der AUFTRAGGEBER - unabhängig von einem Nachweis des AUFTRAGNEHMERS - Anlass hat, die Implementierung geeigneter technischer und organisatorischer Maßnahmen und das Informationssicherheitsmanagement zu prüfen, ist der AUFTRAGGEBER berechtigt, nach vorheriger Abstimmung mit dem AUFTRAGNEHMER zu seinen üblichen Geschäftszeiten ohne Störung des Betriebsablaufs im erforderlichen Umfang Kontrollen, insbesondere durch die Einsichtnahme in die technischen und organisatorischen Maßnahmen und die Einholung von Auskünften, vorzunehmen. Der AUFTRAGGEBER kann eine solche Kontrolle entweder selbst oder durch einen von ihr zu benennende Prüfer durchführen. Der AUFTRAGNEHMER hat das Recht, die Kontrollen zu beaufsichtigen. Er ist dem AUFTRAGGEBER gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

Unterauftrag:

Der AUFTRAGGEBER ist rechtzeitig vor der Beauftragung eines UNTERAUFTRAGNEHMERS zu informieren. Der AUFTRAGGEBER hat das Recht, einer derartigen Beauftragung aus wichtigen Gründen zu widersprechen. Als wichtiger Grund gilt insbesondere, wenn begründete Bedenken bezüglich des ordnungsgemäßen Schutzes der Informationen des AUFTRAGGEBERS bei der Erbringung der Leistungen durch den UNTERAUFTRAGNEHMER bestehen.

Unverzügliche Meldung und Informationspflichten bei Informationssicherheitsvorfällen:

Der AUFTRAGNEHMER hat Unregelmäßigkeiten in der Verarbeitung von Informationen, sowie aller sicherheitsrelevanten Vorfälle, die zu einer Verletzung mindestens eines der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität führen (nachfolgend gemeinsam „Informationssicherheitsvorfälle“) unverzüglich (ohne schuldhaftes Zögern) nach Bekanntwerden zu melden und zu dokumentieren.

Die Dokumentation und Meldung eines Informationssicherheitsvorfalls enthalten mindestens folgende Informationen:

- eine Beschreibung der Art des Informationssicherheitsvorfalls, der betroffenen Informationen, der voraussichtlichen Folgen und der von dem AUFTRAGNEHMER ergriffenen oder beabsichtigten Maßnahmen zur Behebung des Informationssicherheitsvorfalls und der nachteiligen Auswirkungen sowie
- den Namen und die Kontaktdaten des Informationssicherheitsbeauftragten oder eines anderen Ansprechpartners (gemäß Anlage 6).

Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Erfüllung der ihr bei einem Informationssicherheitsvorfall obliegenden Pflichten und erteilt ihr die in diesem Zusammenhang erforderlichen weiteren Informationen.

Kommunikation:

Der AUFTRAGNEHMER richtet Informationen, Meldungen und Fragen zur Informationssicherheit an das Informationssicherheitsmanagement des AUFTRAGGEBERS (gemäß Anlage 6).

Der AUFTRAGNEHMER nennt dem AUFTRAGGEBER einen zentralen Ansprechpartner (inklusive der aktuellen Kontaktdaten), der im Unternehmen des AUFTRAGNEHMERS im Auftrag der Leitungsebene die Aufgabe Informationssicherheit koordiniert, innerhalb des Unternehmens vorantreibt und als Ansprechpartner für den Informationssicherheitsbeauftragten des AUFTRAGGEBERS fungiert (gemäß siehe Anlage 6).

Der Wechsel eines Ansprechpartners wird dem AUFTRAGGEBER über die Aktualisierung der Anlage 6 mitgeteilt.

Ort der Leistungserbringung, Herausgabeverpflichtung von Daten:

Es gelten die Regelungen aus Anlage 7.

Der AUFTRAGNEHMER teilt Änderungen an die in Anlage 6 definierten Ansprechpartner mit und aktualisiert die Anlage 7.

Der AUFTRAGNEHMER stellt sicher, dass im Falle seiner Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit der AUFTRAGGEBER unverzüglich Zugriff auf die im Besitz des AUFTRAGNEHMERS befindlichen Daten des AUFTRAGGEBERS erhält.

NACHWEISE:

Nachstehende Nachweise zum jeweiligen System werden jährlich per 01.12. Per E-Mail an, die in der Anlage 6 genannten Informationssicherheitsbeauftragte Personen durch den AUFTRAGNEHMER versendet und zum Download auf der Homepage des AUFTRAGNEHMERS bereitgestellt.

VR-Bildung GbR:

System	Nachweis	Frequenz
Zentralsystem Bildungsportal	ISO 27001 Zertifikat von Perbility GmbH	Jährlich
Administration und Weiterentwicklung des Learning Management Systems	ISO 27001 Zertifikat von Genoverband e.V. Bestätigung der Berücksichtigung der Sollschutzmaßnahmen inkl. Bericht über wesentliche Abweichungen	Jährlich

Vertragspartner (Regionalakademien):

GenoAkademie GmbH & Co. KG:

System	Nachweis	Frequenz
Buchungsportal (Homepage)	ISO 27001 Zertifikat von Genoverband e.V.	Jährlich
Seminarmanagementsystem	ISO 27001 Zertifikat von U2D Solution GmbH	

Die GenoAkademie GmbH & Co. KG bezieht ihre IT-Systeme über ihren Hauptgesellschafter dem Genoverband e.V. und stellt über dessen ISB und der ISO 27001 Zertifizierung die Einhaltung der Anforderungen sicher.

ABG GmbH:

Die ABG GmbH bezieht ihre wesentlichen IT-Systeme über den Genossenschaftsverband Bayern e.V. (GVB). Dort ist ein Ausschuss zur IT-Sicherheit eingerichtet, der die Funktion eines ISB innehat.

System	Nachweis	Frequenz
Buchungsportal (Homepage)	Bestätigung durch den Beauftragten der VR Bildung GbR (Patrick Te-Strote, Genoverband e.V.).	Jährlich
Seminarmanagement-system		

Genossenschaftsverband Weser-Ems e.V.:

System	Nachweis	Frequenz
Buchungsportal (Homepage)	Bestätigung durch den Beauftragten der VR Bildung GbR (Patrick Te-Strote, Genoverband e.V.).	Jährlich
Seminarmanagementsystem		

Weitere Akademien:

ADG e.V.:

System	Nachweis	Frequenz
Buchungsportal (Homepage)	Bestätigung der Berücksichtigung der Sollschutzmaßnahmen inkl. Bericht über wesentliche Abweichungen durch den ISB der ADG e.V.	Jährlich
Seminarmanagementsystem		

Atruvia AG:

System	Nachweis	Frequenz
Buchungsportal (Homepage)	ISO 27001 Zertifikat Atruvia AG	Jährlich
Seminarmanagementsystem		

Verband der Sparda-Banken e.V.:

System	Nachweis	Frequenz
Seminarmanagementsystem	Bestätigung der Berücksichtigung der Sollschutzmaßnahmen inkl. Bericht über wesentliche Abweichungen durch den ISB des Verbands der Sparda-Banken e.V.	Jährlich

Die aufgeführten Zertifikate und Bestätigungen können für das Jahr 2026 “Informationsnachweise gemäß Anlage 8 Nutzungsvertrag VR-Bildung" (Seite 63 ff.) entnommen werden.

Anhang zur Anlage 8 Informationssicherheit

Begriffsdefinitionen:

Begriff	Beschreibung
Informationssicherheitsvorfall	Ein Informationssicherheitsvorfall (IS-Vorfall) ist ein einzelnes IS-Ereignis oder eine Serie von IS-Ereignissen, verbunden mit Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Prozessen, Aufgaben, Informationen oder informationstechnischen Systemen, bei dem nicht auszuschließen ist, dass ein Schaden für das Unternehmen des AUFTRAGGEBERs oder des AUFTRAGNEHMERs entstehen kann oder bereits entstanden ist.
ISMS	Information Security Management System
ISM	Information Security Management
KPI	Key Performance Indicator

Betroffene Informationen:

Informationsobjekt	Schutzklasse
Personenbezogene Daten • Organisationsdaten, wie Organisationseinheiten, Stellen, Führungszuordnungen, Vertretung – sofern • in geno.HR-PM angelegt • Identifikationsdaten, wie Personalnummer, Geno-User-ID • Mitarbeiterstammdaten: Vor- und Nachname, Titel, Geburtsdatum, Geburtsname • Bilddaten, wie Mitarbeiterfoto – sofern in geno.HR-PM angelegt • Kommunikationsdaten, wie E-Mail, Telefonnummer • Weiterbildungsdaten, wie Anmeldungen/Teilnahmen an Weiterbildungen, WBT-Lernstände – sofern in geno.HR-PM angelegt • - Qualifikationsdaten, wie Qualifikationsnachweise, Qualifikationen – sofern in geno.HR-PM angelegt	S1

Sollschutzmaßnahmen:

Nr.	Kategorie	Beschreibung der Anforderung
ISM-ISR.001	Informationssicherheits-richtlinien	Informationssicherheitsrichtlinien sind festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.
ISM-ISR.002	Informationssicherheits-richtlinien	Der Umgang mit und Zugriffe auf Daten des AUFTRAGGEBERs werden in der Informationssicherheitsrichtlinie berücksichtigt.
ISM-ISR.003	Informationssicherheits-richtlinien	Die erstellten Richtlinien und Arbeitsanweisungen sind mindestens einmal pro Jahr auf ihre inhaltliche Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.
ISM-ISO.001	Informationssicherheitsorganisation	Informationssicherheitsverantwortlichkeiten sind festgelegt und zugeordnet.
ISM-ISO.002	Informationssicherheitsorganisation	Die notwendigen/vorhandenen geteilten Rollen und Verantwortlichkeiten zwischen AUFTRAGNEHMER und AUFTRAGGEBER werden klar definiert und kommuniziert.
ISM-ISO.003	Informationssicherheitsorganisation	Die Definition der Rollen und Verantwortlichkeiten beinhaltet die Zuständigkeiten des AUFTRAGNEHMERs, seinen Zulieferern oder Subdienstleistern und des AUFTRAGGEBERs.
ISM-ISO.004	Informationssicherheitsorganisation	Interessenkonflikte werden vermieden, indem unvereinbare Aufgaben/Tätigkeiten getrennt bzw. nicht von derselben Person durchgeführt werden.
ISM-ISO.005	Informationssicherheitsorganisation	Der AUFTRAGGEBER wird darüber informiert, in welchen Standorten / Ländern Daten des AUFTRAGGEBERs gespeichert, transferiert oder verarbeitet werden.
ISM-ISO.006	Informationssicherheitsorganisation	Es ist sichergestellt, dass der AUFTRAGGEBER in der Lage ist, die Lokationen (Ort/Land) der Datenverarbeitung und -speicherung einschl. der Datensicherungen gemäß der vertraglich zur Verfügung stehenden Optionen festzulegen.
ISM-MT.001	Mobilgeräte und Telearbeit	Es gibt eine für alle Mitarbeiter verpflichtende Richtlinie zum Umgang mit Mobilgeräten.
ISM-MT.002	Mobilgeräte und Telearbeit	Die Verarbeitung und Speicherung von Informationen erfolgten ausschließlich auf freigegebenen Arbeitsgeräten.
ISM-MT.003	Mobilgeräte und Telearbeit	Mobilgeräte sind bei der Nutzung, beim Transport sowie bei der Aufbewahrung gegen unberechtigten Zugriff geschützt (installierte Authentifizierungslösungen).
ISM-MT.005	Mobilgeräte und Telearbeit	Sicherheitsregeln zur Verarbeitung und Speicherung von Informationen während der Heimarbeit sind definiert, umgesetzt und werden kontrolliert.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-MT.006	Mobilgeräte und Telearbeit	Sicherheitsregeln zur Verarbeitung und Speicherung von Informationen an öffentlichen Arbeitsplätzen sind definiert, umgesetzt und werden kontrolliert.
ISM-SSE.001	Schulung und Sensibilisierung	Es ist ein Schulungsprogramm vorhanden, welches zielgruppenorientierte Schulungsinhalte des Informationssicherheitsmanagements für alle Beschäftigten vorgibt.
ISM-SSE.002	Schulung und Sensibilisierung	Die Schulungsinhalte werden mindestens einmal jährlich auf Aktualität und Vollständigkeit überprüft.
ISM-SSE.004	Schulung und Sensibilisierung	Alle Beschäftigten des AUFTRAGNEHMERs nehmen nachweislich in regelmäßigen Abständen an den für sie erforderlichen Schulungsmaßnahmen teil.
ISM-SSE.005	Schulung und Sensibilisierung	Neu eingestellte Beschäftigte sowie Mitarbeiter, die den Tätigkeitsbereich wechseln, werden einer Schulung zur Einhaltung der Informationssicherheitsanforderungen des jeweiligen Bereiches unterzogen.
ISM-SSE.006	Schulung und Sensibilisierung	Mitarbeiter werden zum sicheren Umgang mit Daten des AUFTRAGGEBERs, sowie den aus diesen abgeleiteten Daten, geschult.
ISM-SSE.007	Schulung und Sensibilisierung	Alle Mitarbeiter mit potenziellem Zugriff auf Daten des AUFTRAGGEBERs werden über alle getroffenen Regelungen zum Umgang mit diesen Daten informiert.
ISM-PS.001	Personalsicherheit	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung von Mitarbeitern des AUFTRAGNEHMERs bestehen bleiben, sind festgelegt, den Beschäftigten mitgeteilt und durchgesetzt.
ISM-PS.002	Personalsicherheit	Es ist ein Prozess für das Ausscheiden von Mitarbeitern definiert, in dem festgelegt ist, welche Stellen zu informieren und welche Berechtigungen und Unternehmenswerte einzuziehen sind. Der AUFTRAGGEBER wird informiert, wenn für sie verantwortliche Kontaktpersonen oder Ansprechpartner ausscheiden.
ISM-VW.001	Verantwortlichkeit für Werte	Informationen und andere Werte, die mit Informationen und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind in einem Inventar erfasst, welches stetig aktualisiert wird.
ISM-VW.002	Verantwortlichkeit für Werte	Das Inventar identifiziert eindeutig Daten des AUFTRAGGEBERs, sowie Daten, die aus diesen abgeleitet wurden.
ISM-VW.003	Verantwortlichkeit für Werte	Für alle Werte, die im Inventar geführt werden, gibt es Verantwortliche.
ISM-VW.004	Verantwortlichkeit für Werte	Sicherheitsregeln für den zulässigen Gebrauch von Informationen und anderen Werten, die mit Informationen und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind aufgestellt, dokumentiert und werden kontrolliert.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-VW.005	Verantwortlichkeit für Werte	Mitarbeiter und falls relevant auch Dritte (Subdienstleister) werden hinsichtlich des zulässigen Gebrauchs von Werten und Informationen unterrichtet und darauf verpflichtet.
ISM-VW.007	Verantwortlichkeit für Werte	Es wird sichergestellt, dass alle Beschäftigten und sonstigen Benutzer des AUFTRAGNEHMERs bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die dem AUFTRAGNEHMER oder AUFTRAGGEBER gehören, zurückgeben.
ISM-VW.008	Verantwortlichkeit für Werte	Der AUFTRAGGEBER wird vor der Schließung einer Vereinbarung informiert, wann und wie Assets des AUFTRAGGEBERs bei Beendigung der Vereinbarung zurückgegeben oder gelöscht werden.
ISM-IK.007	Informationsklassifizierung	Vorgaben für die Handhabung von Werten sind entsprechend des Informationsklassifizierungsschemas entwickelt, kommuniziert und umgesetzt.
ISM-HD.001	Handhabung von Datenträgern	Vorgaben für die Handhabung von Datenträgern sind entsprechend des Informationsklassifizierungsschemas umgesetzt.
ISM-ZZS.001	Zugangs- und Zugriffssteuerung	Die Anforderungen an die Zugangs- und Zugriffskontrolle sind durch eine schriftlich fixierte Vorgabe zu regeln.
ISM-ZZS.002	Zugangs- und Zu griffssteuerung	Der Zugriff auf Informationen richtet sich an den geschäftlichen und sicherheitsrelevanten Anforderungen aus und ist in einer entsprechenden Richtlinie festgelegt.
ISM-ZZS.003	Zugangs- und Zugriffssteuerung	Jedes IT-Asset wird in einem Berechtigungskonzept berücksichtigt, das den Umfang und die Nutzungsbedingungen der bereitgestellten Berechtigungen risikoorientiert vorgibt sowie alle Benutzer und deren Rechte ausweist.
ISM-ZZS.004	Zugangs- und Zugriffssteuerung	IT-Komponenten werden nur mit vorheriger Genehmigung in Sicherheitszonen eingebracht bzw. aus Sicherheitszonen entfernt.
ISM-ZZS.005	Zugangs- und Zugriffssteuerung	Rollen, Benutzergruppen und Benutzern werden immer nur die minimal erforderlichen Zugriffsrechte eingeräumt, um ihre fachlichen Aufgaben zu erfüllen („Need-To-Know Prinzip“).
ISM-ZZS.006	Zugangs- und Zugriffssteuerung	Alle Benutzeridentitäten und Berechtigungen von IT-Assets werden mittels eines Identitätsmanagements verwaltet.
ISM-ZZS.007	Zugangs- und Zugriffssteuerung	Benutzer haben ausschließlich Zugang zu denjenigen Diensten, Systemen und Netzwerken, zu deren Nutzung sie ausdrücklich befugt sind.
ISM-ZZS.008	Zugangs- und Zugriffssteuerung	Ein formaler Prozess für die Registrierung und Abmeldung von internen und externen Benutzern ist umgesetzt, um die Zuordnung und den Entzug von Zugangsrechten zu ermöglichen.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-ZZS.009	Zugangs- und Zugriffssteuerung	Nicht personalisierte Accounts (Gruppenaccounts) werden grundsätzlich nicht verwendet.
ISM-ZZS.010	Zugangs- und Zugriffssteuerung	Benutzerkennungen werden eindeutig und somit verwechslungssicher gestaltet (Verwendung personalisierter Accounts).
ISM-ZZS.011	Zugangs- und Zugriffssteuerung	Der Zugriff auf eine Anwendung ist nur möglich, wenn der Benutzer eindeutig identifiziert ist.
ISM-ZZS.012	Zugangs- und Zugriffssteuerung	Jede Benutzerkennung ist genau einer realen / natürlichen Person zugeordnet. Dies gilt auch für Administratorkennungen.
ISM-ZZS.013	Zugangs- und Zugriffssteuerung	System- oder anwendungsbezogene Benutzerkennungen, sogenannte technische User, sind einem Eigentümer (einer realen/natürlichen Person) zugeordnet.
ISM-ZZS.014	Zugangs- und Zugriffssteuerung	Ein formaler Genehmigungs- und Vergabeprozess zur risikobasierten Zuteilung und Entziehung von Benutzerzugängen ist umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.
ISM-ZZS.015	Zugangs- und Zugriffssteuerung	Die Genehmigung und die Einrichtung von Berechtigungen werden nicht durch dieselbe Person durchgeführt.
ISM-ZZS.016	Zugangs- und Zugriffssteuerung	Bei der Genehmigung für die Vergabe und bei der Rezertifizierung von Berechtigungen wird die fachlich verantwortliche Stelle eingebunden.
ISM-ZZS.017	Zugangs- und Zugriffssteuerung	Anträge zur Erlangung oder Änderungen von Berechtigungen auf Anwendungen (inkl. IDV) sind nachvollziehbar zu dokumentieren.
ISM-ZZS.018	Zugangs- und Zugriffssteuerung	Alle persönlichen und technischen Benutzer und alle Berechtigungen eines IT-Assets werden aufgelistet und mindestens jährlich überprüft.
ISM-ZZS.019	Zugangs- und Zugriffssteuerung	Kritische Berechtigungen werden risikoorientiert definiert und dokumentiert.
ISM-ZZS.020	Zugangs- und Zugriffssteuerung	Kritische Berechtigungen werden mindestens halbjährig überprüft
ISM-ZZS.021	Zugangs- und Zugriffssteuerung	Es werden Funktionen bereitgestellt, über welche der AUFTRAGGEBER Benutzerzugriffe auf die eigene Umgebung steuern kann.
ISM-ZZS.022	Zugangs- und Zugriffssteuerung	Privilegierte Berechtigungen und Benutzer werden identifiziert und in einem Berechtigungskonzept dokumentiert.
ISM-ZZS.023	Zugangs- und Zugriffssteuerung	Für administrative Tätigkeiten werden gesonderte Benutzerkonten eingerichtet. Die Kennungen sind logisch von anderen Benutzerkonten zu trennen.
ISM-ZZS.024	Zugangs- und Zugriffssteuerung	Benutzerrechte und -konten, einschließlich Notfall-, Admin und technischen Konten, werden mittels geregelter Verfahren und risikoorientierter Kontrollmechanismen verwendet bzw. eingerichtet.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-ZZS.025	Zugangs- und Zugriffssteuerung	Durchführende Tätigkeiten sind von kontrollierenden Tätigkeiten getrennt.
ISM-ZZS.029	Zugangs- und Zugriffssteuerung	Es gibt klar dokumentierte Regelungen zu Passwortvergabe und -gebrauch, die den Stand der Technik widerspiegeln.
ISM-ZZS.030	Zugangs- und Zugriffssteuerung	Es werden nicht dieselben oder ableitbare Passwörter für berufliche und private Zwecke verwendet.
ISM-ZZS.031	Zugangs- und Zugriffssteuerung	Es werden nicht dieselben oder ableitbare Passwörter für interne und externe Systeme verwendet.
ISM-ZZS.032	Zugangs- und Zugriffssteuerung	Die Prozesse zur Verwaltung und zum Schutz von Authentifizierungsinformationen des AUFTRAGGEBERs werden beschrieben.
ISM-ZZS.033	Zugangs- und Zugriffssteuerung	Die für Unternehmenswerte verantwortlichen Personen überprüfen in regelmäßigen Abständen die Benutzerzugangsrechte auf Aktualität und Erforderlichkeit. Die Frequenz der Überprüfung orientiert sich an der Kritikalität der Zugriffsrechte.
ISM-ZZS.034	Zugangs- und Zugriffssteuerung	Die Zugangs- und Zugriffsrechte aller internen und externen Benutzer, die Zugang bzw. Zugriff auf informationsverarbeitende Einrichtungen des AUFTRAGNEHMERs benötigen, werden bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung unverzüglich entzogen oder bei einer Änderung angepasst.
ISM-ZZS.035	Zugangs- und Zugriffssteuerung	Es wird sichergestellt, dass Authentisierungsmittel nicht weitergegeben, technisch vor Einsichtnahme geschützt sowie ausschließlich verschlüsselt übertragen und gespeichert werden.
ISM-ZZS.036	Zugangs- und Zugriffssteuerung	Temporäre oder voreingestellte Passwörter werden beim ersten Log-In geändert.
ISM-ZZS.037	Zugangs- und Zugriffssteuerung	Der Zugang zu allen Betriebssystemen und Anwendungen wird über ein sicheres (verschlüsseltes) Anmeldeverfahren kontrolliert.
ISM-ZZS.038	Zugangs- und Zugriffssteuerung	Sobald der Verdacht besteht, dass ein Passwort offengelegt wurde, wird das betroffene Passwort geändert und es erfolgt eine Meldung an das Incident Management.
ISM-ZZS.039	Zugangs- und Zugriffssteuerung	Das Niederschreiben oder unautorisierte Abspeichern von Passwörtern ist untersagt.
ISM-ZZS.040	Zugangs- und Zugriffssteuerung	Dem AUFTRAGGEBER werden Mechanismen zur Verfügung gestellt, über die Zugriffe auf Dienste, Funktionen und Daten in der Umgebung kontrolliert werden können.
ISM-ZZS.041	Zugangs- und Zugriffssteuerung	Systeme werden nach mehrfach erfolglosen Anmeldeversuchen automatisch dauerhaft oder für eine definierte Zeit gesperrt.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-ZZS.042	Zugangs- und Zugriffssteuerung	Erfolglose Anmeldeversuche bzw. fehlerhafte Eingaben von Benutzerkennung oder Passwörtern werden protokolliert.
ISM-ZZS.043	Zugangs- und Zugriffssteuerung	Meldung für erfolglose Anmeldeversuche enthalten keine Angabe zu dem Fehler und werden abgelehnt.
ISM-ZZS.044	Zugangs- und Zugriffssteuerung	Sperrungen/Entsperrungen von Benutzerkonten und Passwortrücksetzungen werden protokolliert.
ISM-ZZS.045	Zugangs- und Zugriffssteuerung	Das Anlegen und Löschen von Benutzerkonten wird protokolliert.
ISM-ZZS.046	Zugangs- und Zugriffssteuerung	Die Vergabe, Änderung oder der Entzug von Zugriffsberechtigungen wird protokolliert.
ISM-ZZS.050	Zugangs- und Zugriffssteuerung	Der Zugriff auf Quellcodes von Programmen ist gesichert und auf das erforderliche Mindestmaß an Berechtigten eingeschränkt.
ISM-ZZS.051	Zugangs- und Zugriffssteuerung	Eine angemessene, logische Separierung und Isolierung von Kundendaten, Anwendungen, Betriebssystemen, Speicher und Netzwerk in geteilten Umgebungen ist sichergestellt.
ISM-ZZS.052	Zugangs- und Zugriffssteuerung	Es werden Risiken berücksichtigt, die durch die Möglichkeit entstehen, das Kunden eigene Software in der bereitgestellten (geteilten) Umgebung betreiben.
ISM-ZZS.053	Zugangs- und Zugriffssteuerung	Es wird sichergestellt, dass virtuelle Infrastruktur angemessen gehärtet und mit technischen Maßnahmen abgesichert ist oder durch den AUFTRAGGEBER gehärtet/abgesichert werden kann.
ISM-KG.004	Kryptographie	Der AUFTRAGGEBER wird darüber informiert, in welchen Situationen welche kryptografischen Verfahren eingesetzt werden.
ISM-KG.005	Kryptographie	Der AUFTRAGGEBER wird detailliert darüber informiert, ob sie selbst kryptografische Verfahren in der Umgebung umsetzen kann und welche Anforderungen an diese Verfahren gelten.
ISM-KG.008	Kryptographie	Die verwendeten Schlüssel werden gegen Modifikation, Verlust und Zerstörung geschützt.
ISM-PYS.005	Physische Sicherheit	Der Umgang mit Besuchern wird organisiert und kontrolliert.
ISM-PYS.007	Physische Sicherheit	Alle Räume sind entsprechend der relevanten Gesetze, wie Brandschutzordnung und Arbeitssicherheit, ausgestaltet.
ISM-PYS.016	Physische Sicherheit	Die Verfügbarkeitsanforderungen für Geräte und Betriebsmittel sind bekannt und anforderungsgerecht abgesichert.
ISM-PYS.017	Physische Sicherheit	Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, sowie die Stromverkabelung sind vor Unterbrechung, Störung oder Beschädigung geschützt.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-PYS.019	Physische Sicherheit	Es gibt eine Dokumentation für alle Versorgungsleitungen (mind. Strom, Wasser, Daten, Telefon) im Gebäude oder auf dem dazugehörigen Grundstück, welche regelmäßig und anlassbezogen aktualisiert wird.
ISM-PYS.020	Physische Sicherheit	Es werden Maßnahmen zur Gefahrenabwehr sowie zur Sicherung der Versorgung etabliert und dokumentiert.
ISM-PYS.021	Physische Sicherheit	Geräte und Betriebsmittel werden ordnungsgemäß instandgehalten (Wartung durch geeignetes Fachpersonal), um ihre fortwährende Verfügbarkeit und Integrität sicherzustellen.
ISM-PYS.022	Physische Sicherheit	Geräte, Betriebsmittel, Informationen oder Software werden nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt.
ISM-PYS.023	Physische Sicherheit	Befinden sich Unternehmenswerte außerhalb der Räumlichkeiten des AUFTRAGNEHMERs, werden diese angemessen gegen die verschiedenen Risiken, die damit einhergehen, gesichert.
ISM-PYS.024	Physische Sicherheit	Alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, werden vor ihrer Entsorgung oder Wiederverwendung auf Restdaten überprüft, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software entfernt oder sicher überschrieben worden sind.
ISM-PYS.025	Physische Sicherheit	Es gibt Regelungen, wie unbeaufsichtigte Geräte und Betriebsmittel angemessen vor Diebstahl oder unbefugten Zugriffen geschützt werden müssen.
ISM-PYS.026	Physische Sicherheit	Es gibt eine Richtlinie zur aufgeräumten Arbeitsumgebung (Clear Desk Policy), in der geregelt ist, wie mit Unterlagen und Wechseldatenträgern am Arbeitsplatz zu verfahren ist.
ISM-PYS.027	Physische Sicherheit	Auf Endgeräten sind passwortgeschützte Bildschirmsperren eingerichtet, die bei Abwesenheit verpflichtend aktiviert werden müssen und sich nach einer definierten Zeit selbst aktivieren.
ISM-BS.001	Betriebssicherheit	Die Bedienabläufe für informationsverarbeitende Einrichtungen sind dokumentiert und an alle Benutzer, die diese benötigen, kommuniziert. Die Dokumentation ist für diese Benutzer zugänglich.
ISM-BS.002	Betriebssicherheit	Sollvorgaben für sicherheitsrelevante Einstellungen und Konfigurationen sind für relevante IT-Assets dokumentiert.
ISM-BS.003	Betriebssicherheit	Es ist ein Konfigurationsmanagement-Verfahren definiert, dokumentiert und umgesetzt, welches sicherstellt, dass IT-Assets erfasst, sicher konfiguriert und stetig aktualisiert werden.
ISM-BS.004	Betriebssicherheit	Mitarbeiter werden in neue Systeme, Anwendungen und Verfahren eingewiesen.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-BS.005	Betriebssicherheit	Es ist ein Change-Management Verfahren für die Veränderung von IT-Assets definiert, dokumentiert und umgesetzt.
ISM-BS.006	Betriebssicherheit	Veränderungen am Source Code werden durch eine Versionsverwaltung kenntlich gemacht.
ISM-BS.007	Betriebssicherheit	Der AUFTRAGGEBER wird über alle Änderungen vorab informiert, die Einfluss auf die Umgebung des AUFTRAGGEBERs haben können. Dabei werden alle für den AUFTRAGGEBER relevanten Informationen zur Änderung weitergegeben.
ISM-BS.011	Betriebssicherheit	Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware sind umgesetzt (z.B. Einsatz einer Anti-Virus-Software).
ISM-BS.012	Betriebssicherheit	Schutzmechanismen von IT-Systemen sind so konfiguriert, dass sie durch die Benutzer nicht deaktiviert werden können.
ISM-BS.024	Betriebssicherheit	Dem AUFTRAGGEBER werden Möglichkeiten zur Protokollierung in ihrer Umgebung zur Verfügung gestellt.
ISM-BS.026	Betriebssicherheit	Privilegierte, administrative Aktivitäten werden risikoorientiert protokolliert und kontrolliert. Die Protokolle sind geschützt und werden regelmäßig überprüft.
ISM-BS.027	Betriebssicherheit	Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb eines Sicherheitsbereichs werden mit einer einzigen Referenzzeitquelle synchronisiert.
ISM-BS.028	Betriebssicherheit	Dem AUFTRAGGEBER werden Informationen zur verwendeten Referenzzeitquelle der Cloud-Dienste zur Verfügung gestellt. Zudem wird der AUFTRAGGEBER informiert, ob und wie eine Synchronisation mit lokalen Systemen oder anderen Diensten möglich ist.
ISM-BS.029	Betriebssicherheit	Der AUFTRAGGEBER wird in die Lage versetzt, relevante Aspekte der bereitgestellten Umgebung zu überwachen. Die Überwachung unterliegt einer geeigneten Zugriffskontrolle und stellt sicher, dass keine Informationen anderer Kunden überwacht werden können.
ISM-BS.031	Betriebssicherheit	Die bereitgestellte Umgebung ist mit Fehlerbehandlungs- und Protokollierungsmechanismen ausgestattet. Mittels dieser kann der AUFTRAGGEBER sicherheitsrelevante Informationen über den Sicherheitsstatus der Umgebung sowie den von ihrem bereitgestellten Daten, Dienste oder Funktionen abrufen.
ISM-BS.032	Betriebssicherheit	Falls der AUFTRAGGEBER für die Aktivierung oder Art und Umfang der Protokollierung zuständig ist, stellt der Cloud-Anbieter geeignete Protokollierungsfunktionen bereit.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-BS.033	Betriebssicherheit	Es gibt einen definierten Prozess zur Verteilung und Aktualisierung von Software auf den Systemen.
ISM-BS.034	Betriebssicherheit	Eingesetzte Softwareprodukte beinhalten Maßnahmen zum Schutz vor logischen Datenfehlern, wie Inkonsistenzen und Integritätsverlust.
ISM-BS.035	Betriebssicherheit	Die Sicherheitsfunktion eines Softwareprodukts wird durch unabhängige Prüfer (nicht am Beschaffungsprozess oder Betrieb der Software beteiligt) sichergestellt.
ISM-BS.036	Betriebssicherheit	Softwareprodukte werden vor ihrem produktiven Einsatz hinsichtlich der Erfüllung von Informationssicherheitsanforderungen überprüft und nur zur Nutzung freigegeben, wenn keine Sicherheitsbedenken vorliegen.
ISM-BS.037	Betriebssicherheit	Die Information über technische Schwachstellen verwendeter Informationssysteme wird regelmäßig eingeholt (über Schwachstellenscans und Pentests), die Gefährdung durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen, um das dazugehörige Risiko zu behandeln.
ISM-BS.039	Betriebssicherheit	Alle Security-Patchmanagement- und Pentest-Prozesse sind konkretisiert, umgesetzt und kommuniziert.
ISM-BS.040	Betriebssicherheit	Der AUFTRAGGEBER wird informiert, wie technische Schwachstellen mit Einfluss auf die Umgebung des AUFTRAGGEBERs gemanagt werden.
ISM-BS.041	Betriebssicherheit	Es ist geregelt, wie und welche Softwareinstallationen durch Benutzer erfolgen dürfen.
ISM-BS.038	Betriebssicherheit	Dem AUFTRAGGEBER werden Leitlinien und Empfehlungen zur sicheren Konfiguration, Installation und Nutzung der produktiven Version des Dienstes zur Verfügung gestellt, soweit entsprechende Punkte in der Verantwortung des AUFTRAGGEBERs liegen.
ISM-BSA.003	Betriebssicherheit / ISMS-Audit	Betroffene interne Stellen werden über geplante Audits und damit einhergehende Beeinträchtigungen der Betriebsabläufe rechtzeitig informiert.
ISM-BSA.006	Betriebssicherheit / ISMS-Audit	Feststellungen aus dem Informationssicherheits-Auditbericht werden als Informationssicherheitsrisiken erfasst und behandelt.
ISM-KS.001	Kommunikationssicherheit	Die physische und logische Struktur des Netzwerks ist in Form von Netzwerkplänen dokumentiert.
ISM-KS.002	Kommunikationssicherheit	Das Netzwerk ist segmentiert. Die Segmentierung wird in einem Netzwerkzonenkonzept definiert.
ISM-KS.013	Kommunikationssicherheit	Die Trennung und Kommunikation zwischen den Netzwerkzonen/-segmenten unterliegt angemessenen Sicherheitsmechanismen. Dies impliziert auch die Trennung zwischen dem Netz des AUFTRAGNEHMERs und den Netzen Dritter.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-KS.017	Kommunikationssicherheit	Informationsdienste, Benutzer und Informationssysteme in Netzwerken werden gruppenweise voneinander getrennt gehalten.
ISM-KS.020	Kommunikationssicherheit	Das Netzwerk des AUFTRAGGEBERs ist vom Administrationsnetz des AUFTRAGNEHMERs sowie von den Netzwerken anderer Kunden des AUFTRAGNEHMERs separiert.
ISM-KS.021	Kommunikationssicherheit	Die Informationssicherheitsrichtlinie für virtuelle Netzwerke ist konsistent zur Richtlinie für physische Netzwerke.
ISM-KS.022	Kommunikationssicherheit	Übertragungsrichtlinien, -verfahren und -maßnahmen sind definiert und umgesetzt, um die Übertragung von Informationen für alle Arten von Kommunikationseinrichtungen angemessen zu schützen.
ISM-KS.025	Kommunikationssicherheit	Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation des AUFTRAGNEHMERs an den Schutz von Informationen widerspiegeln, werden identifiziert, regelmäßig überprüft und sind dokumentiert.
ISM-KS.026	Kommunikationssicherheit	Die Eingangs- und Ausgangsschnittstellen, über die die produktive Umgebung angesprochen werden kann, sind angemessen für sachverständiges Personal dokumentiert, sodass diese korrekt verwendet werden können.
ISM-KS.027	Kommunikationssicherheit	Die Kommunikation erfolgt über standardisierte Kommunikationsprotokolle, mit denen die Vertraulichkeit und Integrität der übertragenen Informationen gemäß ihrer Schutzklasse sichergestellt wird.
ISM-SI.001	Sicherheit von Informationssystemen	Informationssicherheitsanforderungen sind in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen und werden berücksichtigt.
ISM-SI.002	Sicherheit von Informationssystemen	Für jeden Dienst und jedes System ist der Schutzbedarf anhand der verarbeitenden Informationen zu analysieren und regelmäßig auf Aktualität und Angemessenheit zu prüfen.
ISM-SI.004	Sicherheit von Informationssystemen	Der AUFTRAGGEBER wird über das generelle Informationssicherheitsniveau der bereitgestellten Umgebung informiert. Dabei werden keine Informationen an Kunden weitergegeben, die für einen potenziellen Angreifer hilfreich wären.
ISM-SEU.007	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Grundsätze für die Anforderungsanalyse sowie Entwicklung und Pflege sicherer Systeme sind definiert, werden regelmäßig aktualisiert und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-SEU.012	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Im Rahmen der Entwicklungen erfolgen funktionale und nicht funktionale Tests, bei denen insbesondere auch die definierten Sicherheitsanforderungen überprüft werden.
ISM-SEU.014	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Ein formales Freigabeverfahren für Änderungen und Entwicklungen von Software und Systemen ist definiert, umgesetzt und wird kontrolliert.
ISM-SEU.015	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Vorgaben für die Auswahl, Nutzung und den Schutz von Testdaten sind definiert, dokumentiert und werden umgesetzt.
ISM-SEU.016	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Personenbezogene Daten und Produktivdaten des AUFTRAGGEBERs werden nicht zu Testzwecken verwendet.
ISM-DM.004	Dienstleistermanagement	Der AUFTRAGNEHMER spezifiziert, welche Informationssicherheitsmaßnahmen im Zusammenhang mit der Umgebung des AUFTRAGGEBERs implementiert werden.
ISM-IM.001	Incident Management	Verantwortlichkeiten und Verfahren für eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sind definiert und etabliert.
ISM-IM.002	Incident Management	Informationssicherheitsvorfälle und deren Behandlung werden nachvollziehbar dokumentiert.
ISM-IM.003	Incident Management	Die Verantwortlichkeit des AUFTRAGNEHMERs, des AUFTRAGGEBERs und die notwendigen Schnittstellen/Prozesse zur Behandlung von Informationssicherheitsvorfällen sind klar definiert.
ISM-IM.004	Incident Management	Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle gemeldet und behandelt.
ISM-IM.005	Incident Management	Dem AUFTRAGGEBER werden Schnittstellen bereitgestellt, mittels welcher Informationen über Sicherheitsvorfälle bidirektional ausgetauscht werden können.
ISM-IM.006	Incident Management	Beschäftigte werden angehalten, jegliche beobachteten oder vermuteten Informationssicherheitslücken in Systemen oder Diensten festzuhalten und zu melden.
ISM-IM.007	Incident Management	Informationssicherheitsereignisse werden anhand festgelegter Kriterien bewertet und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind.
ISM-IM.008	Incident Management	Es sind Prozesse zur Reaktion auf Informationssicherheitsvorfälle definiert, dokumentiert und etabliert.

Nr.	Kategorie	Beschreibung der Anforderung
ISM-IM.013	Incident Management	Der AUFTRAGGEBER wird über Ereignisse informiert, bei denen interne oder externe Mitarbeiter des AUFTRAGNEHMERs lesend oder schreibend auf die verarbeiteten, gespeicherten oder übertragenen Daten zugreifen werden oder bereits zugegriffen haben. Die Information erfolgt gemäß den zusätzlichen vertraglichen Vereinbarungen, spätestens aber 72 Stunden nach dem Zugriff.
ISM-GVA.001	Einhaltung gesetzlicher und vertraglicher Anforderungen	Alle relevanten gesetzlichen, regulatorischen oder vertraglichen Anforderungen sowie das Vorgehen zur Einhaltung dieser Anforderungen sind für jedes Informationssystem und die Organisation des AUFTRAGNEHMERs bestimmt, dokumentiert und werden auf dem neuesten Stand gehalten.
ISM-GVA.002	Einhaltung gesetzlicher und vertraglicher Anforderungen	Der AUFTRAGGEBER wird über alle rechtlichen Zuständigkeiten in Bezug auf den bereitgestellten Cloud-Dienst informiert. Dabei werden auch alle relevanten rechtlichen Anforderungen in Bezug auf die bereitgestellte Umgebung des AUFTRAGGEBERs zur Verfügung gestellt werden.
ISM-GVA.003	Einhaltung gesetzlicher und vertraglicher Anforderungen	Es sind Verfahren definiert und etabliert, um die Einhaltung von gesetzlichen, regulatorischen und vertraglichen Anforderungen hinsichtlich geistiger Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten zu gewährleisten.
ISM-GVA.004	Einhaltung gesetzlicher und vertraglicher Anforderungen	Aufzeichnungen sind gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt.
ISM-GVA.005	Einhaltung gesetzlicher und vertraglicher Anforderungen	Der AUFTRAGGEBER wird informiert, wie Aufzeichnungen in Bezug auf die Nutzung des Dienstes durch den AUFTRAGGEBER geschützt und gespeichert werden.
ISM-GVA.008	Einhaltung gesetzlicher und vertraglicher Anforderungen	Dem AUFTRAGGEBER werden Beschreibungen der kryptografischen Maßnahmen bereitgestellt.
ISM-UIS.003	Überprüfungen der Informationssicherheit	Die Einhaltung der anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstigen Sicherheitsanforderungen bei der Informationsverarbeitung wird regelmäßig überprüft.
ISM-UIS.004	Überprüfungen der Informationssicherheit	Informationssysteme werden regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation des AUFTRAGNEHMERs überprüft.
ISM-HSE.001	Handhabung von staatlichen Ermittlungsanfragen	Es ist ein Prozess zur Handhabung von staatlichen Ermittlungsanfragen definiert. Dabei wird sichergestellt, dass nur Zugriffe mit gültiger Rechtsgrundlage zugelassen werden. Soweit rechtlich möglich, wird der

Nr.	Kategorie	Beschreibung der Anforderung
		AUFTRAGGEBER über Zugriffe auf dessen Daten informiert.
ISM-HSE.002	Handhabung von staatlichen Ermittlungsanfragen	Bei Zugriffen durch Ermittler wird sichergestellt, dass nur die relevanten Daten des betroffenen Kunden und keine Daten anderer Kunden den Ermittlern zugänglich sind.

Anlage 9 Nachhaltigkeitsanforderungen / Verhaltenskodex

Wir als GenoAkademie GmbH & Co. KG bieten ein umfangreiches Dienstleistungsspektrum rund um das Thema Bildung und Personalentwicklung an.

Unseren Erfolg definieren wir nicht nur über das bloße Erreichen des Arbeitsergebnisses, sondern auch über die Art und Weise, wie dies zu Stande kommt. Hier kommen Faktoren, wie Integrität, Vertrauen, Respekt, Gleichberechtigung, Wertschätzung und ein guter Ruf essenziell zum Tragen. Dabei liegt es in der Verantwortung einer/eines jeden Einzelnen ihr/sein Handeln rechts- und gesetzeskonform zu gestalten. Interne Regelungen, die diese Verhaltensweisen vorgeben, sind ein wichtiger Bestandteil zur Förderung einer positiven Unternehmens- und Compliance-Kultur.

Der Verhaltenskodex soll Handlungsorientierung geben, um damit unerwünschten Handlungen vorzubeugen. Er soll dabei helfen, unserer Verantwortung gerecht zu werden sowie Hilfestellung leisten, um die richtigen Entscheidungen zu treffen. Nichtsdestotrotz wird der Verhaltenskodex nicht jede potenzielle Situation abdecken können. Darum ist es umso wichtiger zu sensibilisieren sowie zu kommunizieren, wer die Ansprechpartner*innen bei derartigen vertraulichen Fragestellungen sind.

Geltungsbereich

Der beschriebene Verhaltenskodex gilt für alle Mitarbeitenden, Führungskräfte, Geschäftsführer*innen (im Folgenden: Mitarbeitende) der GenoAkademie GmbH & Co. KG.

Genossenschaftliche Werte leben

Zu den traditionellen genossenschaftlichen Werten zählen Partnerschaftlichkeit, Transparenz, Solidarität, Vertrauen, Fairness und Verantwortung. Nach diesen Werten richten wir unser Handeln aus. Im Fokus unseres Handelns stehen dabei unsere Kund*innen. Dabei sehen wir uns in der Verantwortung, stets eine transparente, kompetente und partnerschaftliche Unterstützung unserer und Kund*innen zu gewährleisten. Die Kommunikation und Zusammenarbeit erfolgen auf Augenhöhe. Durch unsere regionalen Standorte gewährleisten wir eine kompetente und lösungsorientierte Betreuung vor Ort durch vertrauensvolle und verlässliche Ansprechpartner*innen. Vereinbarungen mit unseren Kund*innen schließen wir rechtskonform ab. Wir erfüllen unsere Verpflichtungen und halten uns an die vereinbarten Bedingungen.

Integrität - Unseren Kund*innen gegenüber machen wir wahrheitsgemäße Angaben über unsere Qualifikationen, Leistungen und Kompetenzen. Die Kommunikation erfolgt stets ehrlich und aufrichtig. Wesentliche Informationen werden nicht vorenthalten. Nur auf dieser Grundlage können wir die Basis für eine vertrauensvolle Zusammenarbeit schaffen.

Objektivität – Alle Mitarbeitenden sind zur Objektivität verpflichtet. Mögliche Interessenkonflikte werden vermieden bzw. ihnen ist durch angemessene Maßnahmen entgegenzuwirken.

Fachkompetenz und Sorgfalt – Mitarbeitende sind für uns das höchste Gut. Entsprechend steht die Aus- und Weiterbildung unserer Mitarbeitenden stets im Mittelpunkt, um eine hochwertige Dienstleistung erbringen zu können. Aufträge werden nur angenommen, wenn sie im Rahmen unserer hohen Qualitätsstandards ausgeführt werden können. Wir haben Prozesse und Verfahren eingeführt, die gewährleisten, dass die Aufträge ausschließlich von Mitarbeitenden durchgeführt werden, die über erforderliche Kompetenzen und Qualifikationen verfügen.

Verschwiegenheit – Über Informationen, die wir im Rahmen unserer beruflichen oder geschäftlichen Beziehungen erlangen, wahren wir Verschwiegenheit. Eine Weitergabe dieser Informationen an Dritte, ohne ausdrückliche Genehmigung, ist nicht erlaubt. Eine Ausnahme stellt die Weitergabe von Informationen dar, zu denen wir gesetzlich verpflichtet sind.

Korruptionsprävention

Wir halten uns an die Vorgaben unserer Anti-Korruptionsrichtlinie und nehmen entsprechend keine Zuwendungen an, die unsere Objektivität einer Geschäftsentscheidung beeinflussen oder beeinflussen könnten. Wir haben Maßnahmen implementiert, die Korruption und Kriminalität bekämpfen. Wir lassen uns nicht bestechen und bestechen nicht.

Fairer Wettbewerb

Die Zusammenarbeit mit dem Genoverband e.V. und seiner Tochter- und Netzwerkgesellschaften als auch mit dem Baden-Württembergischen Genossenschaftsverband e.V. und seiner Tochter- und Netzwerkgesellschaften hat keinen Einfluss auf die Erbringung unserer Dienstleistungen. Zudem treffen wir keine Vereinbarungen mit unseren Mitbewerbern, um dadurch den Wettbewerb einzuschränken.

Schutz von Informationen

Im Umgang mit vertraulichen Informationen von Kund*innen und Mitarbeitenden handeln wir verantwortungsbewusst und transparent. Die Verwendung und Verarbeitung von Informationen erfolgt ausnahmslos im Rahmen der geltenden nationalen Gesetze sowie internen Richtlinien und Regelungen. Es werden organisatorische und technische Maßnahmen getroffen, um die Vertraulichkeit von Daten sicherzustellen.

Nachhaltigkeit

Wir tragen eine unternehmerische Verantwortung in Hinblick auf Ökonomie, Umwelt, Soziales (Gesundheit, Sicherheit, Arbeitsschutz) und Unternehmensführung. Der Fokus liegt dabei auf einer effizienten Nutzung begrenzter Ressourcen, der Gesundheit, der Sicherheit und dem Schutz unserer Mitarbeitenden, der

Schonung der Umwelt sowie einer Sensibilisierung für diese Themen. Im Rahmen von kleinen und großen Projekten wurden und werden bereits erfolgreich Maßnahmen umgesetzt. Unsere Beiträge für mehr Nachhaltigkeit sind u. a. eine konsequente Digitalisierung und Förderung des mobilen Arbeitens, ein NewWork-Konzept, ein umfassendes betriebliches Gesundheitsmanagement sowie das Nutzen von regenerativen Energiequellen.

Wir verpflichten uns, Menschenrechtsverletzungen entgegenzuwirken und die Anforderungen aus dem Lieferkettensorgfaltspflichtengesetz einzuhalten. In diesem Zusammenhang stellen wir sicher, dass die UN-Prinzipien für Wirtschaft und Menschenrechte sowie die Kernarbeitsnormen der Internationalen Arbeitsorganisation eingehalten werden.

Gleichberechtigung und Umgang miteinander

Unsere Personalpolitik steht für Gleichberechtigung und Chancengleichheit. Wir bekennen uns zur Diversität und achten Menschen unabhängig von Geschlecht, Alter, Religionszugehörigkeit, Herkunft, ethnischer Zugehörigkeit, sexueller Orientierung, physischer oder psychischer Beeinträchtigung, Weltanschauung (solange nicht im Widerspruch zur freiheitlich demokratischen Grundordnung) und gesellschaftlichem Hintergrund.

Die Förderung von Vielfalt und Chancengleichheit ist uns wichtig. Inklusion und Diversifikation sind für uns daher Herzensanliegen, die wir auch in Projekten sowie im Regelprozess mit Leben füllen, denn wir schätzen und wünschen uns Mitarbeitende mit unterschiedlichsten Fähigkeiten.

Der Umgang miteinander erfolgt fair und auf Augenhöhe. Entschieden stellen wir uns jeder Form von Diskriminierung, Aggression, Rassismus, Sexismus, Chauvinismus und jeglicher weiteren Form menschlichen Fehlverhaltens entgegen und erwarten von allen Agierenden, sich diesem Grundsatz zu verschreiben.

Sanktionen und Konsequenzen

Verstöße gegen den Verhaltenskodex, geltende Rechtsvorschriften sowie interne Regelungen und Richtlinien könnten weitreichende Konsequenzen nach sich ziehen.

Wenn der Verstoß gegen den Verhaltenskodex zugleich einen Verstoß gegen geltende Rechtsvorschriften darstellt, könnte dies unter Umständen zu Geldstrafen oder zu weiteren Sanktionen gegen die GenoAkademie GmbH & Co. KG führen. Auch die Reputation der GenoAkademie GmbH & Co. KG könnte ernsthaft durch Verstöße beschädigt werden.

Ein Verstoß gegen Rechtsvorschriften und/oder den Verhaltenskodex ist entsprechend niemals im Interesse der GenoAkademie GmbH & Co. KG.

Hinweisgebersystem

Unser Handeln ist geprägt von gegenseitigem Respekt und individueller Verantwortung. Wir tolerieren weder Verstöße gegen geltendes Recht noch gegen diesen Verhaltenskodex.

Es besteht zu jeder Zeit die Möglichkeit, vermutete kriminelle Handlungen, gesetzliche Verstöße, Verstöße gegen den Verhaltenskodex sowie gegen regulatorische Anforderungen zu melden.

Wir stellen internen und externen Hinweisgeber*innen verschiedene Meldewege zur Verfügung. Eine Meldung kann auf Wunsch auch anonym erfolgen.

Folgende Wege stehen zur Verfügung, um mögliche Compliance-Verstöße zu melden:

- als Mitarbeiter*in an die direkte Führungskraft
- als externer Dritter an den/die jeweilige/n Ansprechpartner*in der GenoAkademie GmbH & Co. KG
- telefonisch an die Compliance-Beauftragte (Telefonnr. +4951195745266)
- per E-Mail an die Compliance-Beauftragte (whistleblowing@genoverband.de)
- auf Wunsch anonym über das Hinweisgebersystem (Homepage - www.genoverband.de/hinweisgebersystem-whistleblowing)

Hinweise auf mögliche Verstöße werden vertraulich behandelt. Sämtliche Hinweise werden ausnahmslos im Rahmen eines internen Prozesses aufgearbeitet, um den Sachverhalt aufzuhellen.

Hinweisgeber*innen werden nicht benachteiligt, wenn sie mögliche oder tatsächliche Verstöße melden oder Ermittlungen in diesem Zusammenhang unterstützen. Eine Ausnahme von dieser Vorgehensweise stellen Hinweise dar, die missbräuchlich gegeben wurden.

Ansprechpartnerin

Danijela Lemke

Compliance-Beauftragte der GenoAkademie GmbH & Co. KG

Raiffeisenstraße 12, 24768 Rendsburg

Telefon: +4951195745266
E-Mail: danijela.lemke@genoverband.de