Allgemeine Vertragsbedingungen

Grundlagen der Geschäftsbeziehung zwischen
dem Identitätsvermittler VIDIS und Dienstanbieter
Fassung September 2023

1 DEFINITIONEN

1.1 Diensteanbieter.

Anbieter von digitalen Bildungsangeboten, z.B. Schulbuchverlage, E-Learning-Anbieter, Anbieter von Apps im Bildungsbereich, Distributoren von digitalen Bildungsangeboten mehrerer Diensteanbieter.

1.2 Digitales Bildungsangebot.

Jedes Angebot des Diensteanbieters (z.B. Websites, Apps, Lernsoftware), das für den Einsatz im Bildungsbereich konzipiert ist und nicht auf Volljährige beschränkt ist.

1.3 Identitätsanbieter.

Ein Identitätsanbieter ist, wer Identitätsinformationen seiner Nutzer:innen verwaltet. Identitätsanbieter ist diejenige Stelle im Land, die Identitätsinformationen für Nutzer:innen im Land verwaltet und im Rahmen dieser Vertragsbedingungen als dafür beauftragte Behörde des Landes und/oder der an der Pilotphase von VIDIS teilnehmenden Schulen handelt.

1.4 Identitätsanbieter-Daten.

Personenbezogene Daten, die dem Identitätsvermittler von dem Identitätsanbieter im Auftrag des Landes und/oder der an der Pilotphase von VIDIS teilnehmenden Schulen zur Nutzung des Vermittlungsdienstes VIDIS zur Verfügung gestellt werden.

1.5 Identitätsvermittler.

Ein Identitätsvermittler ist, wer ein föderiertes Identitätsmanagement betreibt.

1.6 Lernmittelbezugsvertrag.

Das Vertragsverhältnis zwischen Schulen/Schulträgern/Bildungsträgern/Ländern und einem Diensteanbieter über den Bezug und die Lizenzierung von digitalen Bildungsangeboten für Nutzer:innen.

1.7 Nutzer:innen.

Jede Person, die sich beim Identitätsanbieter rechtmäßig authentifiziert, z.B. Schulträger, Schulleitungen, Lehrer:innen, Schüler:innen, Beschäftigte des Identitätsanbieters, Landes oder Schulträgers oder der Schule.

1.8 Teilnehmer.

Wer entweder als Identitätsanbieter oder als Diensteanbieter an VIDIS angeschlossen ist.

1.9 VIDIS.

VIDIS bedeutet «Vermittlungsdienst für das digitale Identitätsmanagement in Schulen». VIDIS ist ein System, welches Identifizierung, Authentifizierung und Autorisierung zwischen den Bildungsinfrastrukturen der Länder und den Diensteanbietern föderieren kann. Das System ist im Einzelnen in ***Anlage 1*** beschrieben. Weitere Informationen finden sich auf ***www.vidis.schule***.

2 GEGENSTAND DER VERTRAGSBEDINGUNGEN

2.1 Gegenstand der Vertragsbedingungen.

Gegenstand der Vertragsbedingungen ist die Bereitstellung von VIDIS zur Nutzung durch den Diensteanbieter in einem Pilotbetrieb. Teil 1 regelt die grundsätzlichen Voraussetzungen für eine Teilnahme an VIDIS und die erstmalige Herstellung der Anbindung. Teil 2 regelt die Zusammenarbeit im Pilot-Betrieb. Teil 3 enthält Regelungen zur Projektkoordination und Vertragsdurchführung.

2.2 Lizenzen für digitale Bildungsangebote.

Diese Vertragsbedingungen beinhaltet nicht die Vergabe von Lizenzen, aufgrund derer Nutzer:innen das digitale Bildungsangebot des Diensteanbieters nutzen dürfen. Die Berechtigung zum Zugang zu digitalen Bildungsangeboten ist separaten Lernmittelbezugsverträgen vorbehalten. Insbesondere prüft VIDIS nicht selbst, ob Nutzer:innen berechtigt sind, auf ein digitales Bildungsangebot zuzugreifen.

2.3 Anlagen.

Die Anlagen sind in ihrer jeweils gültigen Fassung verbindlicher Bestandteil der Vertragsbedingungen.

Allgemeine Vertragsbedingungen

Grundlagen der Geschäftsbeziehung zwischen
dem Identitätsvermittler VIDIS und Dienstanbieter
Fassung September 2023

Teil 1: Voraussetzungen für eine Teilnahme an VIDIS

3 TEILNAHMEVORAUSSETZUNGEN VIDIS

3.1 **Teilnahmevoraussetzungen**.
Der Diensteanbieter ist während der Laufzeit dieser Vertragsbedingungen zur Teilnahme an VIDIS berechtigt, wenn

a. die technische Anbindung an das digitale Bildungsangebot des Diensteanbieters die technische Prüfung des Identitätsvermittlers besteht (Ziffer 4), und

b. der Diensteanbieter aktuelle Angaben und Dokumentationen auf der Plattform des Identitätsvermittlers hinterlegt hat (Ziffern 5), und

c. das über VIDIS zugängliche digitale Bildungsangebot des Diensteanbieters inhaltliche, rechtliche und insbesondere datenschutzrechtliche Grundanforderungen erfüllt (Ziffer 6). Der Lernmittelbezugsvertrag mit dem Diensteanbieter kann daneben weitergehende Anforderungen enthalten.

3.2 **Prüfung, Verantwortlichkeit des Diensteanbieters.**
Der Identitätsvermittler prüft vor Freischaltung für den Pilotbetrieb die Teilnahmevoraussetzungen in dem in Ziffern 4 – 6 beschriebenen Umfang. Die Verantwortlichkeit des Diensteanbieters zur Einhaltung der Teilnahmevoraussetzungen wird durch die Prüfung nicht berührt.

3.3 **Prüfergebnis.**
Bei erfolgreicher Prüfung erteilt der Identitätsvermittler dem Diensteanbieter per Textform die Freigabe zur Teilnahme an VIDIS. Mit erfolgreicher Freigabe hat der Diensteanbieter das Recht, sich während der Laufzeit der Vertragsbedingungen in der Außenkommunikation und vor allem in Verhandlungen über Lernmittelbezugsverträge mit „geeignet für Nutzung mit VIDIS im Rahmen der Pilotphase" zu bezeichnen. Für die Verwendung der Marken und Designs des Identitätsvermittlers gilt Ziffer 8.3. entsprechend.

3.4 **Änderungen beim Diensteanbieter.**
Änderungen beim Diensteanbieter oder in dem digitalen Bildungsangebot, die nicht völlig unerhebliche Auswirkungen auf die technische Anbindung, die Abläufe beim Einloggen in das digitale Bildungsangebot oder dessen rechtliche Bewertung nach Ziffer 6 und insbesondere die Konformität mit dem Datenschutz haben, machen eine erneute, ggfs. abgekürzte Freigabeprüfung erforderlich. Der Identitätsvermittler hat das Recht hierzu die Teilnahme des Diensteanbieters auszusetzen. Es gilt die Ziffer 11. Der Diensteanbieter wird den Identitätsvermittler bei solchen Änderungen unverzüglich in Kenntnis setzen.

3.5 **Kosten der Prüfung.**
In der vertragsgegenständlichen Pilotphase trägt der Identitätsvermittler die Kosten der Prüfung.

3.6 **Testzugang.**
Der Diensteanbieter gewährt dem Identitätsvermittler für die Laufzeit der Vertragsbedingungen unentgeltliche, vollwertige Zugänge für Testzwecke zu dem an VIDIS angeschlossenen oder vorgesehenen digitalen Bildungsangebot des Diensteanbieters. Die Zugänge für Testzwecke erlauben es dem Identitätsvermittler, die jeweiligen Rollen der Nutzer:innen unbeschränkt und mit gleichen Rechten einzunehmen. Der Identitätsvermittler wird diese Zugänge für Testzwecke ausschließlich für vertragsbedingungsgemäße Zwecke, insbesondere weitere Prüfungen verwenden.

4 TECHNISCHE PRÜFUNG

4.1 **Technische Anbindung.**
Für die Nutzung von VIDIS sind auf den Systemen und in dem digitalen Bildungsangebot des

Diensteanbieters technische Voraussetzungen gemäß ***Anlage 2*** herzustellen. Dies ist Sache des Diensteanbieters. Übergabepunkt sind die Schnittstellen zu VIDIS.

4.2 Prüfungsumfang.

Der Identitätsvermittler prüft die Geeignetheit, Integrität, Funktionsfähigkeit und Sicherheit der technischen Anbindung und der Einbindung der Funktionalitäten von VIDIS gemäß dem Verfahren in ***Anlage 7***. Mit der Prüfung ist keine Gewährsübernahme für die technische Anbindung im Leistungsbereich des Diensteanbieters verbunden.

5 DOKUMENTATION

5.1 Upload.

Der Diensteanbieter verpflichtet sich, die Dokumente gemäß ***Anlage 8*** auf der Plattform des Identitätsvermittlers zur Verfügung zu stellen. Diese Dokumente dürfen durch den Identitätsvermittler nach Rücksprache mit dem Diensteanbieter öffentlich zugänglich gemacht werden. Für die Dokumentation besteht eine Aktualisierungspflicht nach Ziffer 9.4.

5.2 Prüfungsumfang.

Der Identitätsvermittler prüft die Vollständigkeit, nicht jedoch die inhaltliche Richtigkeit und Zweckmäßigkeit der hochgeladenen Dokumente.

6 GRUNDANFORDERUNGEN AN DIGITALEN BILDUNGSANGEBOTE

6.1 Inhaltliche Grundanforderungen.

Der Diensteanbieter verpflichtet sich, nur ein solches digitales Bildungsangebot für eine Anbindung an VIDIS bereitzustellen, das folgende inhaltliche Grundanforderungen erfüllt:

a. Das digitale Bildungsangebot dient dem Bildungsauftrag, indem es
- einen klaren, didaktischen, pädagogischen oder schulischen Zweck über das Lehren, Lernen oder deren Verwaltung im schulischen Bereich erfüllt, und
- primär für den Einsatz in der formalen Bildung konzipiert ist, und
- für allgemeinbildende Schulen und/oder berufliche Schulen in öffentlicher Trägerschaft vorgesehen ist, und
- bei Lern- und Lehrmitteln Anforderungen der einschlägigen Lehrpläne und Richtlinien inhaltlich, didaktisch und methodisch Rechnung trägt.

b. Das digitale Bildungsangebot berücksichtigt die Vorgaben aus den Beschlüssen der Ständigen Konferenz der Kultusminister der Länder (KMK), soweit diese auf das digitale Bildungsangebot ihrem Sinn und Zweck nach anwendbar sind.

c. Die Inhalte in dem digitalen Bildungsangebot erfüllen nach dem jeweils anwendbaren Landesrecht die Zulassungsvoraussetzungen für Lehr- und Lernmittel.

6.2 Rechtmäßigkeit des digitalen Bildungsangebots.

Der Diensteanbieter verpflichtet sich, nur ein solches digitales Bildungsangebot an VIDIS anzubinden, das rechtmäßig ist. Hierzu gehört insbesondere:

a. Das digitale Bildungsangebot bzw. dessen Inhalte verstoßen nicht gegen die verfassungsgemäße Ordnung des Bundes und der Länder, das Strafrecht und enthält keinerlei rassistische, extremistische, volksverhetzende oder das Unrecht des Nationalsozialismus leugnende oder verharmlosende Inhalte.

b. Das digitale Bildungsangebot ist werbefrei, es sei denn, eine konkrete Werbung ist nach den einschlägigen Bestimmungen für Lehr- und Lernmittel ausnahmsweise zulässig. Aus dem digitalen Bildungsangebot darf für Nutzer:innen der Benutzer:innengruppe Schüler:innen nicht auf Zielseiten verlinkt werden, die Werbung enthalten. Nutzer:innen der Benutzer:innengruppe Schüler:innen dürfen keine kostenpflichtigen Zusatzangebote (In-App-Verkäufe), „Freemium-Geschäftsmodelle“ oder kostenpflichtige

Upgrade-Angebote angeboten werden.

c. Das digitale Bildungsangebot ist jugendmedienschutzrechtlich unbedenklich.

6.3 Grundanforderungen im Datenschutz.

Der Diensteanbieter verpflichtet sich zum datenschutzrechtkonformen Umgang mit den personenbezogenen Daten der Nutzer:innen. Darüber hinaus gelten folgende Grundanforderungen:

a. Die personenbezogenen Daten der Nutzer:innen dürfen ausschließlich dafür verwendet werden, das digitale Bildungsangebot verfügbar zu machen (Zweckbindung).

b. Das digitale Bildungsangebot enthält für Nutzer:innen der Benutzer:innengruppe Schüler:innen keinerlei Einwilligungsabfrage, gleich für welchen Zweck.

c. Die Verlagerung der Datenverarbeitung in ein Land, das nicht Mitglied der Europäischen Union oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ist, oder Land, für das kein Angemessenheitsbeschluss der Europäischen Kommission gemäß Artikel 45 DSGVO vorliegt, ist unzulässig. Andere Lösungen zum Drittstaatentransfer bedürfen einer schriftlichen Freigabe des Verantwortlichen für die Datenverarbeitung und des Identitätsvermittlers.

d. Die Erstellung von Nutzerprofilen erfolgt nur innerhalb des vom Diensteanbieter selbst betriebenen digitalen Bildungsangebots und wird nicht mit weiteren Datenquellen zusammengeführt (Datentrennung).

e. Die Einbindung fremder Dienste oder Inhalte in das digitale Bildungsangebot (inklusive Cookies, Libraries, Fonts etc), die nicht in einem genehmigten Auftragsverarbeitungsverhältnis zum Diensteanbieter stehen, ist untersagt.

f. Der Diensteanbieter verarbeitet ausschließlich personenbezogene Daten der Nutzer:innen aus denjenigen Kategorien, die zwischen den Parteien in ***Anlage 3*** verbindlich definiert wurden und nur zu den in ***Anlage 3*** bestimmten Verwendungszwecken. Überdies garantiert der Diensteanbieter, nur solche personenbezogenen Daten von Nutzer:innen aus VIDIS zu verarbeiten, für die eine Rechtsgrundlage nach dem Lernmittelbezugsvertrag besteht. Der Identitätsvermittler trifft technische Vorkehrungen gegen Fehlübermittlungen.

g. (leer)

h. Für die bei dem Diensteanbieter gespeicherten Daten der Nutzer:innen hat der Diensteanbieter festzulegen, für welchen Zeitraum eine Aufbewahrung bzw. eine Speicherung zu erfolgen hat. Nach Ablauf der Aufbewahrungsfrist bzw. Speicherdauer ist für eine Löschung zu sorgen.

i. Ungeachtet vorstehenden Absatzes sind die personenbezogenen Daten der Nutzer:innen, 18 Monate ab letzten Nutzungsvorgang, zu löschen.

j. Der Diensteanbieter gewährt den Nutzer:innen ein Recht auf Datenübertragbarkeit (analog Art. 20 DSGVO) und stellt Funktionalitäten bereit, um dieses ausüben können. Sofern die Nutzer:innen die direkte Übertragung der Daten an eine andere Person verlangen, erfolgt dies nur, soweit es technisch machbar ist.

6.4 Prüfungsumfang, Prüfungsbefugnis.

Der Identitätsvermittler prüft die inhaltlichen Grundanforderungen an die digitalen Bildungsangebote (Ziffer 6.1) und deren Rechtmäßigkeit (Ziffer 6.2) auf Basis der zur Verfügung gestellten und frei verfügbaren Informationen nach billigem Ermessen kursorisch auf Plausibilität. Gleiches gilt für die Grundanforderungen zum Datenschutz und insbesondere einzelne Datenschutzklauseln, sofern einzelne Elemente hiervon nicht Teil der technischen Prüfung nach Ziffer 4 sind.

Weitergehend kann eine datenschutzrechtliche Prüfung durch einen vom Identitätsanbieter bzw. dem Land oder dem Identitätsvermittler beauftragten Dienstleister anhand eines zu erstellenden Prüfkatalogs erfolgen. Der Diensteanbieter räumt hiermit dem Identitätsvermittler die Befugnisse zur datenschutzrechtlichen Prüfung – auch durch beauftragte Dritte - im identischen Umfang ein, in welchem der Diensteanbieter diese dem Identitätsanbieter und/oder dem Land im Rahmen des Vertrages über eine Auftragsverarbeitung einräumt.

7 FOLGEN BEI FEHLEN VON TEILNAHMEVORAUSSETZUNGEN

7.1 **Kein Pilot-Betrieb.**
Ohne erfolgreiche Freigabe zur Teilnahme (Ziffer 3.3) darf der Diensteanbieter die Funktionalitäten von VIDIS nicht im Pilot-Betrieb nutzen.

7.2 **Nachträgliche Kenntniserlangung einer fehlenden Teilnahmefähigkeit.**
Erlangt der Identitätsvermittler während der Laufzeit der Vertragsbedingungen nachträglich Kenntnis darüber, dass der Diensteanbieter Pflichten nach Ziffern 4 – 6 verletzt, gilt folgendes abgestufte Verfahren:

a. Bei kleineren oder leicht behebbaren Verstößen gibt der Identitätsvermittler dem Diensteanbieter einen Hinweis in Textform mit der Bitte, das Problem in situationsangemessener Frist (Regelfall: 14 Tage) zu lösen.

b. Erfolgt keine Abhilfe, oder liegt ein schwerwiegender Verstoß vor, mahnt der Identitätsvermittler den Diensteanbieter schriftlich unter Fristsetzung ab. Die Abmahnung wird dem Auftraggeber des Lernmittelbezugsvertrags und dem Anbieter des Landessystems zur Kenntnis gegeben.

c. Erfolgt innerhalb der Frist keine Abhilfe, nimmt der Identitätsvermittler Rücksprache mit dem Auftraggeber des Lernmittelbezugsvertrags und dem Anbieters des Landessystems. Sofern sich hieraus keine begründeten Einwände ergeben, widerruft der Identitätsvermittler die Freigabe und stellt dem Diensteanbieter die VIDIS-Funktionen für einen Pilot-Betrieb nicht weiter zur Verfügung.

d. In Notfällen, insbesondere zum Schutz der Nutzer:innen, kann der Identitätsvermittler die Anbindung des Diensteanbieters nach Ziffer 11.3 vorübergehend suspendieren.

e. Die Geltendmachung weiterer gesetzlicher Rechte aufgrund der Pflichtverletzung bleibt unberührt.

Teil 2: Zusammenarbeit im Pilot-Betrieb

8 BEREITSTELLUNG VON VIDIS

8.1 **Bereitstellung, Caveat.**
Der Identitätsvermittler verpflichtet sich, während Laufzeit der Vertragsbedingungen VIDIS entsprechend den Spezifikationen in ***Anlage 2*** auf eigenen Systemen vorzuhalten und dem Diensteanbieter dessen Nutzung über die freigegebene technische Anbindung (Ziffer 4) zu ermöglichen. Diese Bereitstellungspflicht betrifft nur die Funktionalitäten von VIDIS auf den Systemen des Identitätsvermittlers. Eine vollständige Identitätsvermittlung setzt überdies Leistungen, eine ausdrückliche Freigabe zur Datenweiterleitung und eine technische Anbindung der Identitätsanbieter bzw. der Länder voraus, zu denen diese gegenüber dem Identitätsvermittler nicht verpflichtet sind. Von der Leistungspflicht des Identitätsvermittlers sind daher diejenigen Leistungen für eine Identitätsvermittlung ausgenommen, die von Identitätsanbietern bzw. den Ländern zu erbringen sind.

8.2 **Verfügbarkeit.**
VIDIS soll grundsätzlich 24/7 zur Verfügung stehen. Für den vertragsgegenständlichen Pilotbetrieb schuldet der

Identitätsvermittler keine spezifische Verfügbarkeit. Der Identitätsvermittler wird sich jedoch noch besten Kräften bemühen, die für den späteren Folgebetrieb vorgesehene Verfügbarkeit zu realisieren.

8.3 **Lizenz für VIDIS Marke.**
Der Identitätsvermittler erteilt dem Diensteanbieter mit erfolgreicher Freigabe (Ziffer 3.3) das Recht, die Wort-/Bildmarke „VIDIS" und die VIDIS-Designs für die Dauer der Vertragsbedingungen für vertragsbedingungsgemäße Zwecke zu nutzen und in das digitale Bildungsangebot einzubinden. Die Darstellung von VIDIS hat dem VIDIS Brandbook gemäß ***Anlage 4*** zu entsprechen.

8.4 **Standardisierungen, Änderungen und Erweiterungen.**
Der Identitätsvermittler übernimmt im Rahmen des „Digitalpakts Schule" die Rolle, technische, organisatorische, datenschutzrechtliche und inhaltliche Standards für VIDIS und das Netzwerk der Teilnehmer und angeschlossenen Bildungsangeboten zu entwickeln und laufend zu verbessern. Aus diesem Grunde kann der Identitätsvermittler nach folgender Maßgabe Änderungen an dem eigenen Dienst, an den technischen Spezifikationen, den Datenkategorien und den inhaltlichen und datenschutzrechtlichen Teilnahmevoraussetzungen vornehmen:

a. Für den Diensteanbieter vorteilhafte oder neutrale Änderungen kann der Identitätsvermittler nach mindestens 14-tägiger Vorankündigung einseitig umsetzen. Insbesondere in diese Kategorie fallen bloße Konkretisierungen der vertraglich vereinbarten Leistungen einschließlich der Leistungsbeschreibung von VIDIS, Fehlerbereinigung an eingesetzter Software, geringfügige Anpassungen der Schnittstellen, geringfügige Änderungen der Architektur, geringfügige Funktionserweiterungen oder Funktionsänderungen und Performanceverbesserungsmaßnahmen.

b. Der Identitätsvermittler kann jederzeit Produktupdates vornehmen, solange für den Diensteanbieter die Option der rückwärtskompatiblen Anwendbarkeit von VIDIS bis zur Vertragsbeendigung besteht

c. Sonstige Änderungen sind möglich, wenn sie gesetzlich verpflichtend oder von den für die Schulaufsicht zuständigen Stellen der Ländern angeordnet sind, wenn sie der technischen Optimierung, der Verbesserung der Sicherheit, des Datenschutzes oder der User Experience für Nutzer:innen dienen. Solche Änderungen werden dem Diensteanbieter mindestens sechs Wochen zuvor in Textform angekündigt und die Gelegenheit zur Stellungnahme gegeben. Dem Diensteanbieter steht, sofern durch den Identitätsvermittler keine Option der rückwärtskompatiblen Anwendbarkeit von VIDIS bis zur Vertragsbeendigung besteht, ein Recht zur außerordentlichen Kündigung zum Zeitpunkt des Wirksamwerdens einer Änderung zu. Erfolgt seitens des Diensteanbieters sechs Wochen nach Änderungsmitteilung keine Kündigung, wird die Änderung zum Zeitpunkt des Wirksamwerdens Bestandteil der Vertragsbedingungen. Der Identitätsvermittler wird den Diensteanbieter auf diese Folge in der Änderungsmitteilung ausdrücklich hinweisen.

8.5 **Support.**
Der Identitätsvermittler unterstützt den Diensteanbieter bei der Umsetzung der technischen Anbindung mit organisatorischer und technischer Beratung während der üblichen Bürozeiten. Der Identitätsvermittler leistet keinen Endkundensupport für Nutzer:innen.

8.6 **Einsatz Dritter.**
Der Identitätsvermittler kann sich zur Erfüllung seiner vertraglichen Dienstleistung auch anderer Personen bedienen.(Erfüllungsgehilfen). Datenschutzrechtliche Bestimmungen bleiben hiervon unberührt.

9 LEISTUNGEN DES DIENSTEANBIETERS

9.1 **Keine Nutzungspflicht, keine Exklusivität.**

Vorliegende Vertragsbedingungen begründen für den Diensteanbieter keine Verpflichtung zur Teilnahme an VIDIS. Eine solche kann sich aus anderen Rechtsverhältnissen (z.B. dem Lernmittelbezugsvertrag) ergeben. Dem Diensteanbieter bleibt es nach diesen Vertragsbedingungen unbenommen, weitere Optionen zum Einloggen neben VIDIS bereitzuhalten.

9.2 **Teilnahmeberechtigung.**

Der Diensteanbieter ist zur Teilnahme an VIDIS im Pilot-Betrieb unter der Bedingung berechtigt, dass er die Teilnahmevoraussetzungen nach Ziffern 4 – 6 auch nach Zugang des Prüfergebnisses (Ziffer 3.3) laufend erfüllt.

9.3 **Datenqualität.**

Der Diensteanbieter stellt mit angemessenen Maßnahmen sicher, dass die Nutzungsdaten, die zwischen dem Identitätsanbieter und Diensteanbietern direkt übertragen werden, richtig und aktuell sind.

9.4 **Aktualisierung.**

Der Diensteanbieter verpflichtet sich, die nach Ziffer 5.1 bereitgestellten Dokumente stets unter Führung eines Change Logs aktuell zu halten und Änderungen im Regelfall binnen 14 Tagen auf die Plattform des Identitätsvermittlers hochzuladen.

10 VERGÜTUNG, KOSTEN

10.1 **Unentgeltlichkeit.**

Für die Dauer dieser Vertragsbedingungen über einen Pilotbetrieb stellt der Identitätsvermittler VIDIS unentgeltlich bereit.

10.2 **Kosten.**

Jeder trägt die Kosten der technischen Anbindung im eigenen Leistungsbereich selbst.

11 LEISTUNGSSTÖRUNGEN

11.1 **Wartungen.**

Betrieb und Nutzbarkeit von VIDIS können durch Wartungen unterbrochen werden. Wartungen finden grundsätzlich in Zeiten außerhalb der Schulzeiten (08:00 – 16.00 Uhr) statt und werden dem Diensteanbieter mindestens 14 Tage im Voraus , angekündigt, sofern kein unaufschiebbarer Grund vorliegt (akuter Fehler, Sicherheitsupdates)..

11.2 **Informationspflichten, Störungsmeldung.**

Die Vertragsparteien informieren sich gegenseitig unverzüglich über Vorkommnisse im eigenen Betriebsbereich, die Rückwirkungen auf den Betrieb oder die Nutzung von VIDIS haben können (z.B. Störungen, Stromabschaltungen, Lastabschaltungen, Datensicherheitsverstöße). Im Falle der Störung von VIDIS leitet der Identitätsvermittler unverzüglich nach der Störungsmeldung Maßnahmen zur Entstörung ein.

11.3 **Suspendierung.**

Der Identitätsvermittler kann die technische Anbindung des Diensteanbieters vorübergehend sperren, wenn

a. er rechtlich hierzu verpflichtet wird, etwa per einstweiliger Verfügung oder durch eine Anweisung des Auftraggebers des Lernmittelbezugsvertrags bzw. der datenschutzrechtlich verantwortlichen Stelle;

b. aufgrund substantiierter Hinweise die Sperrung wegen Gefahrenverzugs notwendig erscheint, um Schaden vom Diensteanbieter, dem Identitätsvermittler, den Identitätsanbietern oder Nutzer:innen abzuwenden, und die Gefahr nicht kurzfristig durch eine Kontaktaufnahme mit dem Diensteanbieter abgewendet werden kann.

c. es Änderungen nach Ziffer 3.4 gibt.

In jedem Fall wird der Identitätsvermittler den Diensteanbieter unverzüglich über die Sperrung in Kenntnis setzen.

12 HAFTUNG, FREISTELLUNG

12.1 **Haftung bei schwerem Verschulden.**
Die Vertragspartner haften einander bei Vorsatz oder grober Fahrlässigkeit für alle von ihnen sowie ihren gesetzlichen Vertretern oder Erfüllungsgehilfen verursachten Schäden unbeschränkt.

12.2 **Haftung bei Verletzung von Leben, Körper, Gesundheit.**
Bei leichter Fahrlässigkeit haften die Vertragspartner im Fall der Verletzung des Lebens, des Körpers oder der Gesundheit unbeschränkt.

12.3 **Haftung bei leichter Fahrlässigkeit.**
Im Übrigen haftet ein Vertragspartner nur, soweit er eine wesentliche Vertragspflicht verletzt hat. Wesentliche Pflichten aus den Vertragsbedingungen sind solche Pflichten, die für die Erreichung des Vertragsziels von besonderer Bedeutung sind, ebenso alle diejenigen Pflichten, die im Fall einer schuldhaften Verletzung dazu führen können, dass die Erreichung des Vertragszwecks gefährdet wird. In diesen Fällen ist die Haftung auf den Ersatz des vorhersehbaren, typischerweise eintretenden Schadens beschränkt. Ziffern 12.1 und 12.2 bleiben unberührt.

12.4 **Freistellung.**
Der Diensteanbieter hält den Identitätsvermittler von sämtlichen Schäden frei, die dem Identitätsvermittler aus einem Verstoß gegen die Pflichten aus Ziffern 4 – 6 entstehen, es sei denn, der Diensteanbieter hat diesen Verstoß nicht zu vertreten.

Teil 3: Projektkoordination und Vertragsdurchführung

13 LAUFZEIT UND KÜNDIGUNG

13.1 **Beginn, Befristung.**
Das Vertragsverhältnis beginnt mit Unterzeichnung und endet am 30. Juni 2024, ohne dass es einer Kündigung bedarf. Die Vertragsparteien werden rechtzeitig über einen Vertrag für den Folgebetrieb verhandeln.

13.2 **Ordentliche Kündigung.**
Das Vertragsverhältnis kann von jeder Vertragspartei mit einer Frist von einem Kalendermonat jeweils zum Monatsende ordentlich gekündigt werden.

13.3 **Außerordentliche Kündigung.**
Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor:

a. wenn eine Vertragspartei trotz einer schriftlichen Abmahnung wiederholt eine wesentliche Pflichten aus den Vertragsbedingungen verletzt, eine fortdauernde Verletzung der Vertragsbedingungen innerhalb angemessener Frist nicht abstellt oder deren Folgen nicht beseitigt. Als wesentliche Pflicht der Vertragsbedingungen gelten insbesondere Teilnahmevoraussetzungen nach Ziffern 4 – 6;

b. wenn der Identitätsvermittler die Entscheidung trifft, VIDIS einzustellen.

13.4 **Schriftform.**
Die Kündigung bedarf der Schriftform.

13.5 **Abwicklung.**
Nach einer Kündigung werden die Parteien alle Dokumente und Unterlagen und ggfs. Software, die von der anderen Partei im Rahmen im Zusammenhang mit VIDIS erhalten wurden, zurückgeben und bestätigen, dass alle Kopien davon vorbehaltlich gesetzlicher Aufbewahrungspflichten vernichtet wurden. Der Diensteanbieter wird alle personenbezogenen Daten der Nutzer:innen löschen, es sei denn, für eine weitere Verarbeitung besteht eine Rechtsgrundlage. VIDIS wird nach Kündigung ohne Beteiligung des Diensteanbieters fortgeführt.

14 PROJEKTKOORDINATION UND ALLGEMEINE GRUNDSÄTZE DER ZUSAMMENARBEIT

14.1 **Kommunikation und Koordination.**
Die Vertragsparteien benennen gegenseitig einen Ansprechpartner und einen Stellvertreter, die innerhalb der Geschäftszeiten erreichbar sind und kurzfristig Entscheidungen herbeiführen können. Die Ansprechpartner bei Vertragsschluss sind in ***Anlage 5*** bezeichnet.

14.2 **Technische Informationen.**
Der Identitätsvermittler wird dem Diensteanbieter die technischen Informationen zur Verfügung stellen, die für die Teilnahme an VIDIS notwendig sind; die Informationen sind von dem Diensteanbieter abzurufen.

14.3 **Gegenseitige Unterstützung, Wohlverhalten.**
Die Vertragsparteien verpflichten sich zu einer engen und fairen Kooperation. Sie wissen, dass das Projekt nur bei gemeinsamer Anstrengung erfolgreich durchgeführt werden kann.

14.4 **Öffentliche Verlautbarungen.**
Die Vertragsparteien werden sämtliche Presseinformationen, Presseerklärungen und sonstige öffentliche Verlautbarungen über den Abschluss oder die Durchführung dieser Vertragsbedingungen nur nach vorheriger gegenseitiger Abstimmung abgeben, herausgeben oder auf sonstige Art und Weise Dritten zur Verfügung stellen.

14.5 **Vertraulichkeit.**
Die Vertragsparteien verpflichten sich, alle ihnen vor oder bei der Vertragsdurchführung von der jeweils anderen Vertragspartei zugehenden oder bekanntwerdenden Gegenstände (z.B. Software, Unterlagen, Informationen), die rechtlich geschützt sind oder Geschäfts- oder Betriebsgeheimnisse enthalten oder als vertraulich bezeichnet sind, auch über das Vertragsende hinaus vertraulich zu behandeln, es sei denn, sie sind ohne Verstoß gegen die Geheimhaltungspflicht öffentlich bekannt. Die Vertragsparteien verwahren und sichern diese Gegenstände so, dass ein Zugang durch Dritte ausgeschlossen ist. Die Vertraulichkeitsverpflichtung gilt nicht für Informationen, die der Öffentlichkeit zum Zeitpunkt des Vertragsschlusses allgemein zugänglich sind oder nach Vertragsschluss ohne Verschulden der jeweils anderen Vertragspartei zugänglich gemacht werden. Sie gilt ebenfalls nicht für Informationen, die sich bereits vor Offenlegung durch die offenlegende Vertragspartei im Besitz der anderen Vertragspartei befanden oder durch diese unabhängig entwickelt wurden.

15 SCHLUSSBESTIMMUNGEN

15.1 **Verhaltens- und Leistungskontrolle**
VIDIS wird nicht zu Zwecken der Leistungskontrolle, des Leistungsvergleichs oder der Leistungsbemessung der Arbeitnehmer eingerichtet oder genutzt.

15.2 **Anwendbares Recht.**
Auf das Vertragsverhältnis findet deutsches materielles Recht Anwendung.

15.3 **Gesamter Vertrag, Schriftform.**
Diese Vertragsbedingungen einschließlich seiner Anlagen stellt die gesamte Vereinbarung der Vertragsparteien in Bezug auf den Vertragsgegenstand dar. Nebenabreden bestehen nicht. Änderungen oder Ergänzungen dieses Vertrags und Anlage 6 bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung dieses Schriftformerfordernisses. Änderungen oder Ergänzungen der Anlagen 1 bis 5 sowie 7 bis 8 bedürfen zu ihrer Wirksamkeit der Schriftform oder Textform.

15.4 **Abtretungsverbot.**
Die Abtretung von Ansprüchen aus diesem Vertragsverhältnis ist ohne Zustimmung der

anderen Vertragspartei ausgeschlossen.

15.5 **Salvatorische Klausel.** Sollte eine Bestimmung dieser Vertragsbedingungen unwirksam oder undurchsetzbar sein oder werden, bleiben die übrigen Bestimmungen dieser Vertragsbedingungen hiervon unberührt. Die unwirksame und undurchsetzbare Bestimmung ist von den Vertragsparteien durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, die dem Zweck der ersetzten Bestimmung möglichst nahekommt.

15.6 **Gerichtsstand.** Ausschließlicher Gerichtsstand ist, sofern nicht eine Norm zwingend einen anderen Gerichtsstand anordnet, München.

ANLAGENVERZEICHNIS.

ANLAGE 1

Beschreibung des VIDIS Vermittlungsdienstes

ANLAGE 2

Spezifikationen zu Schnittstellen/Integration

ANLAGE 3

Spezifikationen
zu den Datensätzen

ANLAGE 4

VIDIS Brandbook

ANLAGE 5

Ansprechpartner

ANLAGE 6

(leer)

ANLAGE 7

Technische Prüfung
der Anbindung

ANLAGE 8

Dokumentation

Allgemeine Vertragsbedingungen

Grundlagen der Geschäftsbeziehung zwischen
dem Identitätsvermittler VIDIS und Dienstanbieter
Fassung September 2023

VIDIS

Anlagen 1- 8

Anlage 1:

Beschreibung des VIDIS Vermittlungsdienstes

Disclaimer: Pilotphase - Änderungen möglich

Einleitung - Was ist der VIDIS-Dienst?

Die Lehr- und Lernwirklichkeit hat sich im Zuge der Digitalisierung enorm gewandelt. Das Internet hält vielfältige Angebote aus dem Bildungsbereich bereit. Auf technischer Ebene wird dabei häufig von Diensten bzw. Services gesprochen. Bereitgestellt werden diese Angebote von Anbietern aus dem öffentlichen und privaten Bereich. Für eine wachsende Anzahl an Diensten sind zur Nutzung persönliche Konten erforderlich, beispielsweise um Klassengemeinschaften abbilden und individuelle Lernstände speichern zu können.

Zur Anmeldung benötigen Benutzer:innen (user) individuelle Zugangsdaten. So steigt mit der Anzahl der genutzten Angebote auch die Anzahl der persönlichen Zugangsdaten (meist Name und Passwort) oder auch "Digitale Identitäten" genannt.

Um den Zugang zu digitalen Diensten zu vereinfachen, haben sich in den letzten Jahren Identity-Management-Systeme (IDM) verbreitet. IDM verwalten digitale Identitäten und stellen zentral für mehrere Angebote ("Service Provider", "SP") Nutzerkonten als Identity Provider (IdP) bereit . Diese Architektur verringert einigen Aufwand auf Anwenderseite aber auch auf Seite der Anbieter.

Durch den Einsatz gemeinsam genutzter IDM Systeme wird auch technisch der einmalige Login ermöglicht (Single-Sign-On), um im Anschluss auf alle Angebote ohne erneute Anmeldung zugreifen zu können.

Im Idealfall existiert nur ein Identity Provider, der alle Service Provider anbindet. In der Praxis ist das aber selten der Fall und funktioniert meist nur innerhalb einer mehr oder weniger geschlossenen Gruppe bzw. Organisation.

Die vielen verschiedenen Gruppen oder Organisationen, in denen Identity Provider (IdP) und Service Provider (SP) agieren, können aber ihrerseits grundsätzlich ebenfalls untereinander kommunizieren und Informationen über Identitäten teilen. Dies wird als technische **Föderation** bezeichnet und es werden hierbei mehrere IdP mit vielen SP einfach und schnell miteinander verbunden. Um dies zu gewährleisten, müssen Standards und Regeln organisatorischer und technologischer Art mit dem Ziel vereinbart werden, dass Benutzer:innen mit nur einer einzigen Anmeldung - und einer digitalen Identität - alle ihnen grundsätzlich zugänglichen Dienste innerhalb dieser Föderation nutzen können.

Das Medieninstitut der Länder

Der VIDIS-Dienst baut die technische und kommunikative Infrastruktur für eine solche Föderation von IDPs und SPs im deutschen Bildungsbereich auf.

Überblick aktueller Stand

Seit Februar 2022 ist das Pilotsystem erfolgreich in Betrieb.

Ziele

- Detaillierte Anforderungen für den Projektverlauf generieren.
- Organisatorische Prozesse etablieren.
- Feedback von Stakeholdern einholen und damit die Architektur ggfs. anpassen.

Aufbau

- Komponenten VIDIS-Dienst
    - VIDIS-IAM Pilotsystem (https://aai.vidis.schule/auth/realms/vidis/.well-known/openid-configuration)
    - VIDIS-IAM Pilot Testsystem (https://aai-test.vidis.schule/auth/realms/vidis/.well-known/openid-configuration)
    - VIDIS-IAM Pilot Dev-System (intern)
    - VIDIS-Button zum späteren Zeitpunkt auf (repo.vidis.schule)
- Anbindung Pilotphase
    - Mehrere Landesportale (Stand: 12.07.2022)
        i. BayernCloud IDM (mebis)
        ii. SuBITI Bremen
        iii. Schulcampus RLP
        iv. Online-Schule-Saarland
    - Ausgewählte Bildungsangebote
- Livesysteme bzw. produktive Systeme
    - Echtdaten
- Single-Sign-On-Technologie für Anbieter: OpenID Connect
- Single-Sign-On-Technologie Länder: OpenID Connect / SAML 2.0

Wie nutze ich den VIDIS-Dienst?

Aktuell ist die Anmeldung aus einem Portal oder über einen VIDIS-Login möglich.

Einstieg über ein Landesportal

Der Einstieg aus einem Portal kann über verschiedene Wege erfolgen. Beispielsweise über das Dashboard eines Portals (Abbildung 1), eine Mediathek (Abbildung 2), ein Lern-Management-System oder andere Oberflächen. Der VIDIS-Dienst selbst ist keine Anwendung, die für die Benutzer:innen sichtbar ist. VIDIS läuft als Vermittlungsdienst zischen Angeboten (SP) und Identity Providern (IdP). Im Vordergrund stehen die digitalen Bildungsangebote (Service Provider), die von den Benutzer:innen ausgewählt werden können und über einen einfachen Zugang (Single-Sign-On) erreichbar sind.

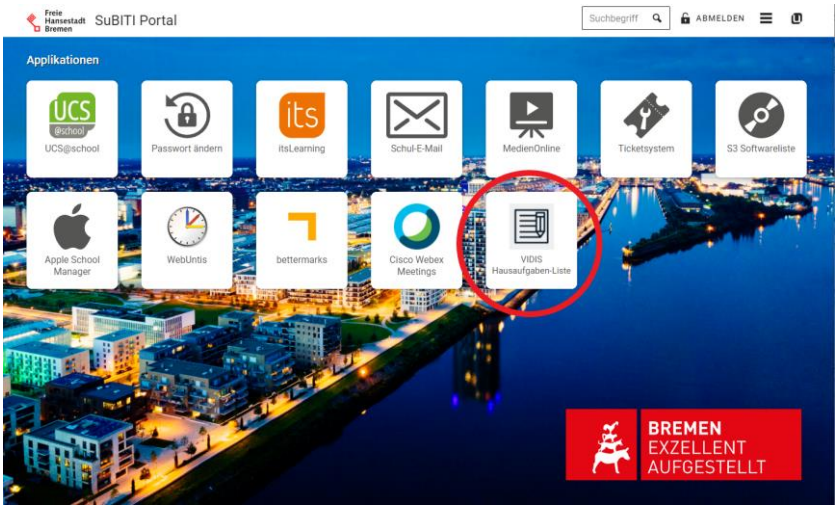


Abbildung 1: Dashboard

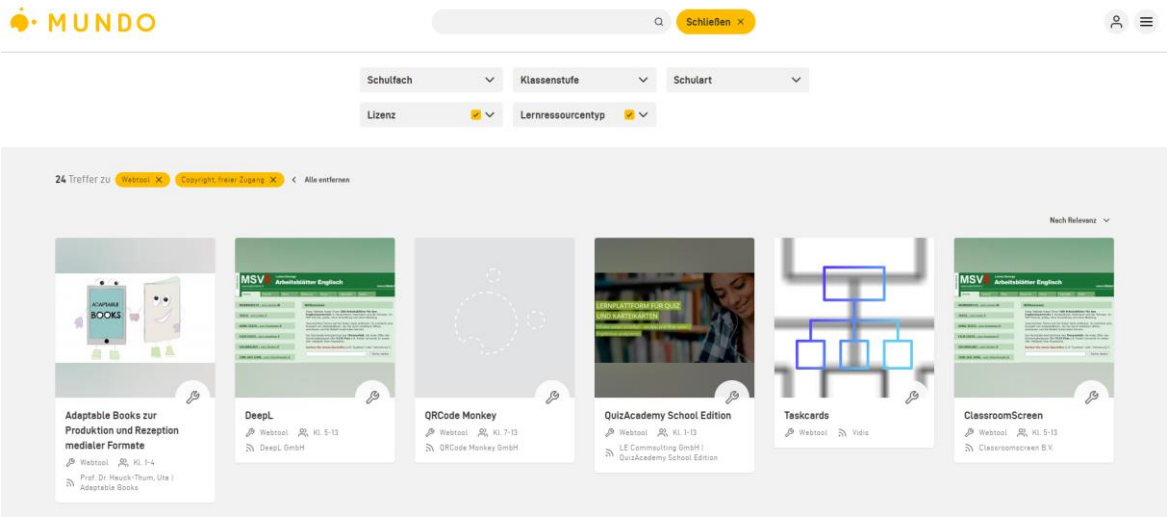


Abbildung 2: Mediathek

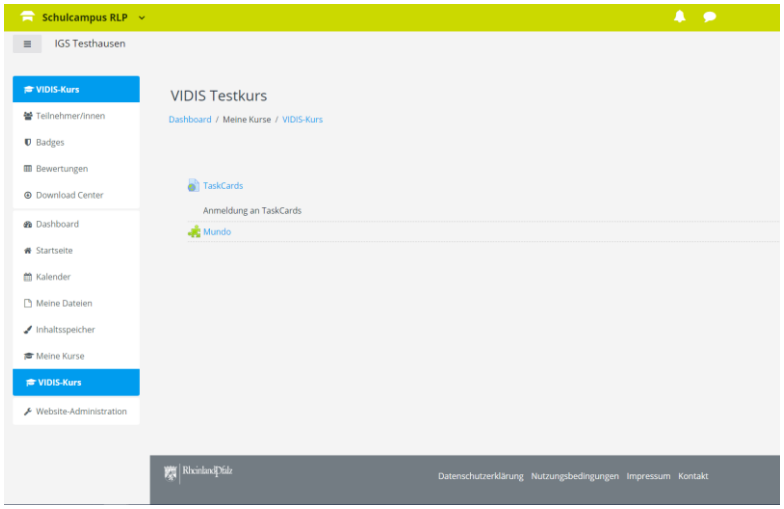


Abbildung 3: Lern-Management-System

Einstieg über den VIDIS-Login

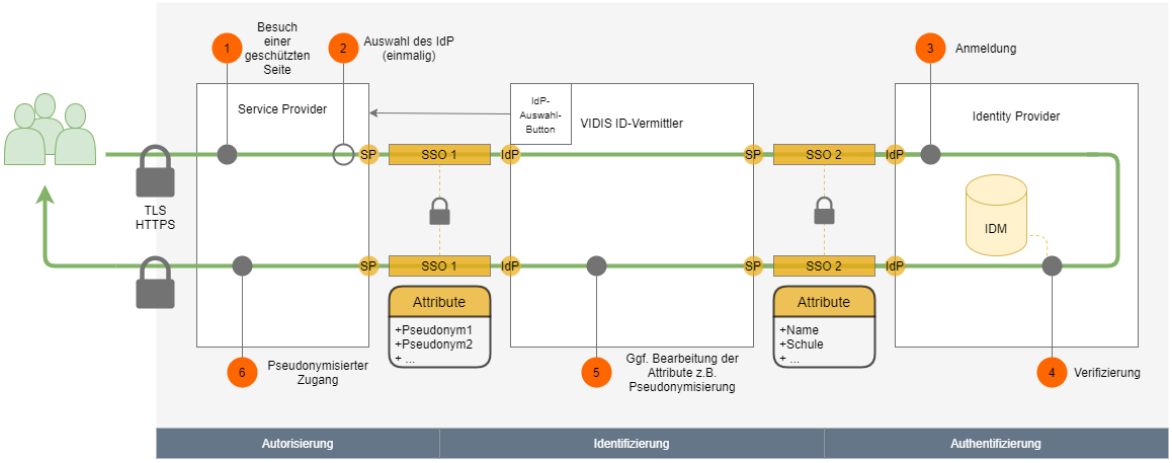
Perspektivisch wird es einen VIDIS-Login geben, dieser wird vom VIDIS-Dienst zur Einbindung im Anmeldebereich der Service Provider bereitgestellt.

Beim erstmaligen Klick auf den Button erscheint zunächst eine Suchmaske. In dieser Suchmaske können Benutzer:innen das eigene Landesportal suchen und auswählen. Diese Auswahl speichert der VIDIS-Dienst über einen Cookie, sodass beim nächsten Aufruf keine Auswahl des Landesportals mehr notwendig ist.

Beim Klick auf das Landesportal werden Benutzer:innen zur Anmeldung des Landesportals geleitet. Dort sind die Anmeldedaten einzugeben und zu bestätigen und die Benutzer:innen werden anschließend zurück zum Bildungsangebot weitergeleitet (Redirect).

Was passiert beim Aufruf

Anmeldeprozess: Übersicht



1. Der Prozess beginnt mit dem Besuch einer geschützten Seite eines digitalen Bildungsangebots.
    a. Der Service Provider leitet die Benutzer:innen entweder direkt an den ID-Vermittler weiter oder bietet eine Login-Seite auf der die Besucher/innen den "VIDIS-Button" wählen können.
2. Benutzer:innen wählen ihre Heimatorganisation (IdP) innerhalb eines Dialog aus (anhand des Namens der Schule oder des Schulportals).
3. Die Benutzer:innen werden vom ID-Vermittler an ihren "IdP" weitergeleitet und geben dort ihre Anmeldedaten an.
4. Die Anmeldedaten werden vom IDM des IdP abgeglichen, verifiziert und die Benutzer:innen werden zurück an den ID-Vermittler geleitet.
5. Im ID-Vermittler erfolgen das Attribut-Mapping, die Pseudonymisierung und die Weiterleitung an den Service Provider.
6. Der Service Provider erhält das OK und kann den pseudonymen Zugang ermöglichen.

Anmeldeprozess: Datenflussdiagramm

⚠ Übermittlung ausschließlich, sofern Anbieter eines Angebots:

1. Hinreichend den Informationspflichten nachgekommen sind (z.B. Dokumentation der Zwecke der Verarbeitungstätigkeiten, TOM, etc.).
2. Eine darüber hinausgehende Selbstverpflichtung (Akkreditierungsvertrag) unterzeichnet haben.

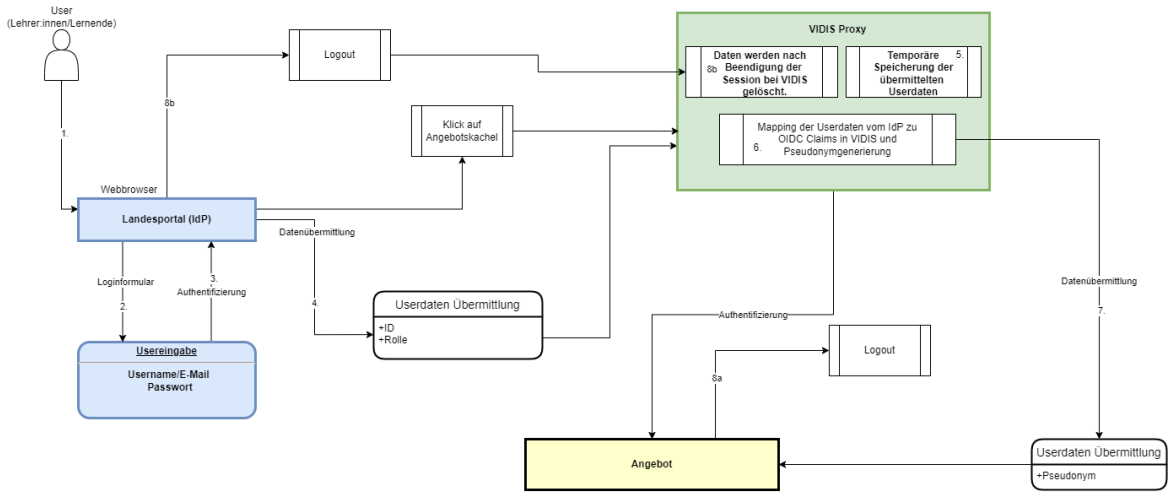
Datenmodell

⚠ Mit Ländern abgestimmter Vorschlag. Unter Vorbehalt weiterer rechtlicher Klärungen.

Das Datenmodell ist in Anlage 3 dargestellt.

Datenfluss Pilotphase Teil 1 (ab Q3'22)

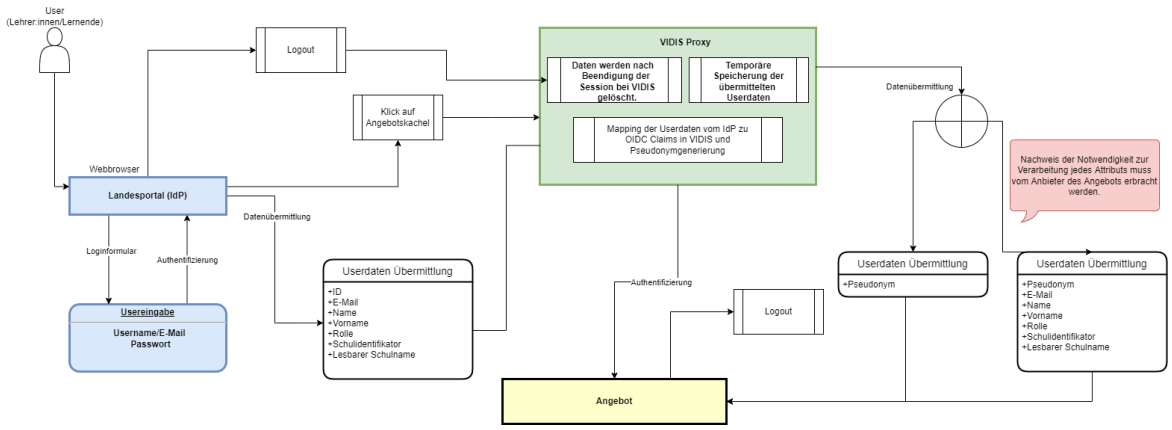
⚠ Vorschlag. Unter Vorbehalt weiterer rechtlicher Klärungen.



1. Benutzer:in ruft über den Browser sein Landesportal auf und klickt auf Login
2. Er gibt seine Anmeldedaten in Loginformular ein
3. Benutzer:in wird authentifiziert
4. Die Userdaten werden übermittelt und bei VIDIS eine Session gestartet
5. Das VIDIS-System speichert die Daten temporär für die Session.
6. Daten werden in VIDIS gemapped und ein Pseudonym wird generiert
7. Das Pseudonym wird als einziges Attribut an das Angebot übermittelt
8. Logout
    a. Beim Logout im Angebot bleibt die Session auf dem Landesportal und VIDIS aktiv
    b. Beim Logout auf dem Landesportal werden die Daten bei VIDIS gelöscht

Datenfluss Pilotphase Teil 2 (ab ca. Q4'22 geplant) "Kern-Datensatz"

⚠ Vorschlag. Unter Vorbehalt weiterer rechtlicher Klärungen.

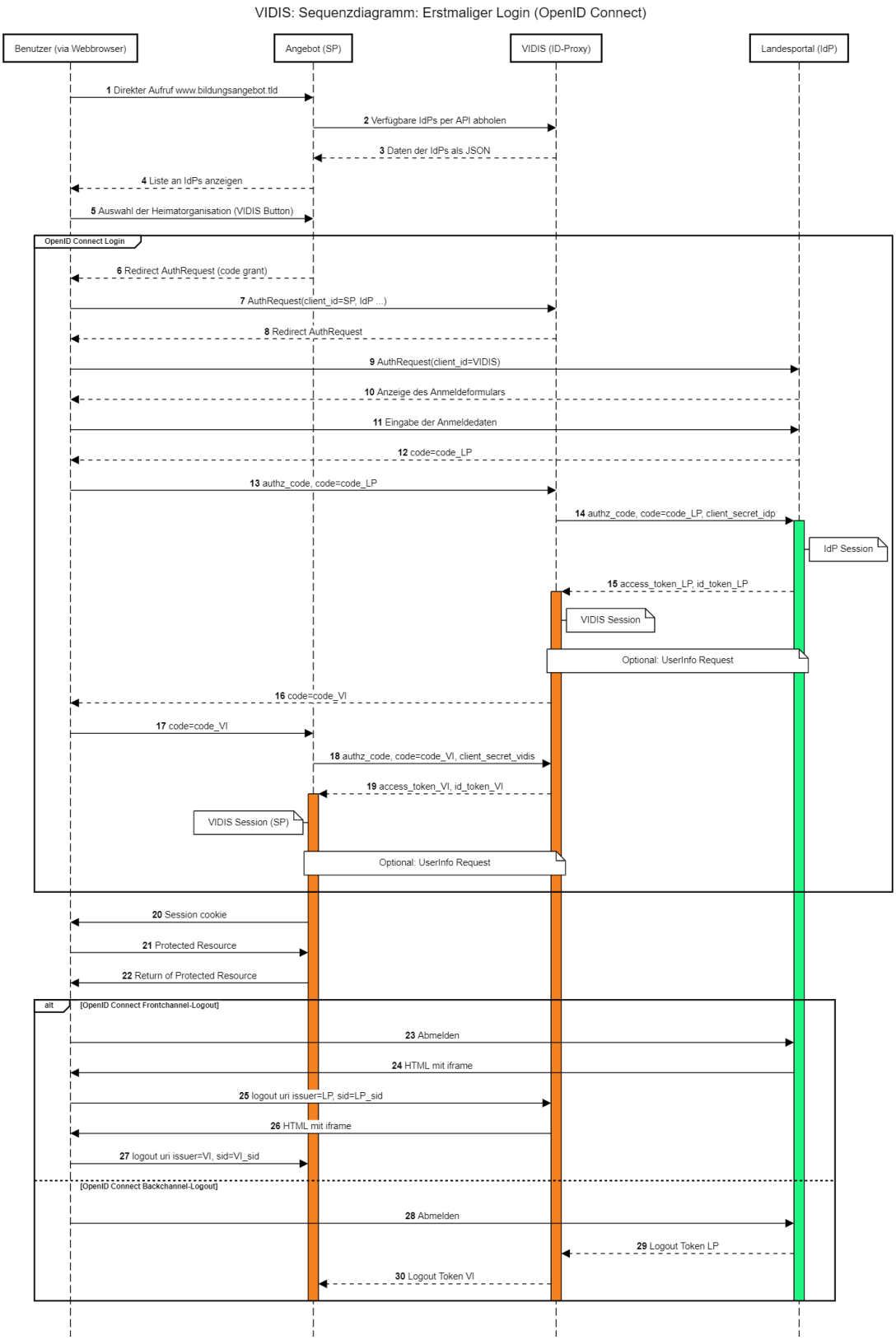


1. User ruft über den Browser sein Landesportal auf und klickt auf Login
2. Er gibt seine Anmeldedaten in Loginformular ein
3. Benutzer:in wird authentifiziert
4. Die Userdaten werden übermittelt und bei VIDIS eine Session gestartet
5. VIDIS speichert die Daten temporär für die Session.
6. Daten werden in VIDIS gemapped und ein Pseudonym wird generiert
7. Es gibt zwei Möglichkeiten
    a. Das Pseudonym wird als einziges Attribut an das Angebot übermittelt
    b. Zusätzlich werden weitere Attribute an das Angebot übermittelt. Kern wird dabei die Frage sein, dass eine Notwendigkeit zur Verarbeitung nachgewiesen wird.
8. Logout
    a. Beim Logout im Angebot bleibt die Session auf dem Landesportal und VIDIS aktiv
    b. Beim Logout auf dem Landesportal werden die Daten bei VIDIS gelöscht

Anmeldeprozess: Sequenzdiagramm

Hier am Beispiel eines IDPs (wie in Abschnitt 2.1 erklärt).

Nach dem Klick auf "Anmelden" werden die Tokens generiert über OpenID Connect (OIDC) an den VIDIS Provider geschickt. Mit dem access_token kann dieser nun auf die Userinfo zugreifen.



(Diagramm auf sequencediagram.org)

Das UML Sequenzdiagramm veranschaulicht, wie sich Benutzer:innen bei einem Angebot anmelden, das über OIDC an VIDIS angebunden ist. Der dahinterliegende IdP ist hierbei an VIDIS als ID-Proxy ebenfalls über OIDC angebunden.

In einem ersten Schritt wird durch die Benutzer:innen die Webseite eines Bildungsangebots (Beispiel: www.bildungsangebot.tld) im Browser aufgerufen

(1) Um auf nicht öffentliche, geschützte Ressourcen zuzugreifen, müssen sich die Benutzer:innen zunächst authentisieren. Für die Darstellung der verfügbaren Identity Provider (IdPs) werden diese über eine API des VIDIS ID-Proxys abgefragt **(2)**, in strukturierter Form zurückgeliefert **(3)** und schließlich auf der Loginseite gerendert **(4).**

Das Bildungsangebot muss hierzu eine (beliebige) OIDC Library integrieren und VIDIS als IdP konfigurieren, da der VIDIS ID Proxy gegenüber des Bildungsangebots (Webanwendung) als Identity-Provider wahrgenommen wird.

Durch die Bereitstellung einer JS Library für die Frontend Komponente des VIDIS Buttons, wird eine einheitliche Darstellung und Funktionsweise in allen Angeboten erreicht. Hierzu findet bereits vor der ersten Userinteraktion initial ein Abruf über die VIDIS Webserver statt, um die entsprechende JS Datei laden zu können.

Da der Authorization Code Flow verwendet wird, ist eine reine JS Implementierung auf der Angebotsseite nicht ausreichend und das Angebot muss serverseitig ein OIDC Library integrieren. Aus Sicherheitsgründen wird der "Implicit Code-Flow" nicht verwendet.

Wenn für das Bildungsangebot nur ein IdP konfiguriert ist, lässt sich diese manuelle Auswahl der Heimatorganisation durch sie Benutzer:innen auch überspringen. Hierzu würde innerhalb des Angebots bei der Button Integration an die URL des Authorization Endpunkts ein entsprechender Parameter angehängt. Am Beispiel des aktuell im PoC verwendeten Open-Source-Produkt Keycloak könnte das wie folgt aussehen:

https://vidis-proxy-id.de/auth?client_id=my-id&scope=openid&redirect_uri=https://bildungsangebot.de&response_type=code&state=T0lEQw==&kc_idp_hint=idp_alias_xyz
Damit wäre dann die entsprechend parametrisierte Heimatorganisation vorausgewählt.

Sind mehrere Auswahlmöglichkeiten vorhanden, wählen die Benutzer:innen in Schritt **(5)** den IdP ihrer Heimatorganisation aus und erhlten via Redirect **(6)** die URL für den Authentication Request beim VIDIS ID-Proxy **(7)**. Ein Authentication Request (https://openid.net/specs/openid-connect-core-1_0.html#AuthRequest) in OpenID Connect (OIDC) ist ein OAuth 2.0 Authorization Request (vom Typ Authorization Code Grant (https://datatracker.ietf.org/doc/html/rfc6749#section-4.1)), erweitert um eine Authentisierung der Endbenutzer:innener beim Authorization Server.

Im Falle eines föderierten OIDC Flows erkennt der VIDIS ID-Proxy, dass nicht er selbst die Usererdaten verwaltet, sondern ein extern angebundener IdP. Daher sendet der VIDIS ID-Proxy die URL für die föderierte Anfrage zurück zum Browser **(8)**, der nun den Authentication Request direkt beim IdP ihrer Heimatorganisation der Benutzer:innen stellt **(9)**. Der IdP präsentiert den Benutzer:innen eine Webseite (**10),** auf der sie ihre Zustimmung ("user consent") geben oder ablehnen können. Im Positivfall authentisieren sich die Benutzer:innen beim IdP **(11)**, der die

Anmeldedaten validiert und einen Authorization Code an den Browser zurücksendet **(12)**. Dieser kann nur einmal verwendet werden, um ein gültiges Access Token (https://datatracker.ietf.org/doc/html/rfc6749#section-1.4) zu bekommen.

Über den Browser wird nun ein Request zusammen mit der Authorization Code an den VIDIS ID-Proxy gesendet **(13)**, der die Anfrage an den IdP weiterleitet, inklusive einem Client Secret, das auf IdP Seite geprüft wird **(14)**. Der IdP validiert die Anfrage inkl. Client Secret und sendet im Erfolgsfall ein Access Token und ein ID Token (https://openid.net/specs/openid-connect-core-1_0.html#IDToken) an den VIDIS ID-Proxy zurück **(15)**.

Aus Datenschutzgründen wird für jeden registrierten Client ein anderes, nicht zurückverfolgbares Subject (sub) für die Benutzer:innen verwendet (Pairwise Identifier Algorithm (https://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg). Dadurch ist ein "Profiling" der Benutzer:innen durch Anbieter mehrere Bildungsangebote hinweg nicht möglich.

In Schritt **(16)** sendet der VIDIS ID-Proxy einen Authorization Code an den Browser, der diesen an den SP weiterleitet **(17),** um seinerseits einen Request beim VIDIS ID-Proxy zu stellen **(18)**. Nach Prüfung sendet dieser ein Access Token und ein ID Token an den SP **(19).**

Sollte die Anwendung weitere Userdaten benötigen, können optional mit Hilfe des Access Tokens beim UserInfo Endpunkt (https://openid.net/specs/openid-connect-core-1_0.html#UserInfo) weitere "Claims" wie z.B. Klassenstufe oder Schulart der authentifizierten Benutzer:innen abgefragt werden.

Nachdem der Browser pseudonymisierte VIDIS Daten und Anwendungsdaten vom Angebot (SP) bekommen hat **(20)** und eine Session zwischen Browser und Angebot (SP) besteht**,** können die Benutzer:innen auf geschützte Ressourcen zugreifen **(21)**, indem der Access Token von VIDIS im Header der Anfrage übermittelt wird **(22).**

Um sich beim Angebot (SP) anzumeden, sendet der Browser eine entsprechende Anfrage an den zuständigen IdP **(23),** der ein Logout Token zunächst an den VIDIS ID-Proxy über den Frontchannel sendet **(24)**. Dies setzt den Einsatz von iFrames voraus und setzt die Anpassung der "Content Security Policy" voraus.

Empfohlen wird alternativ der Backchannel Logout **(28)** , der seinerseits dem Angebot (SP) ein Logout Token **(30)** über den zuvor angeforderten Logout Token des Landesportals **(29)** übermittelt.

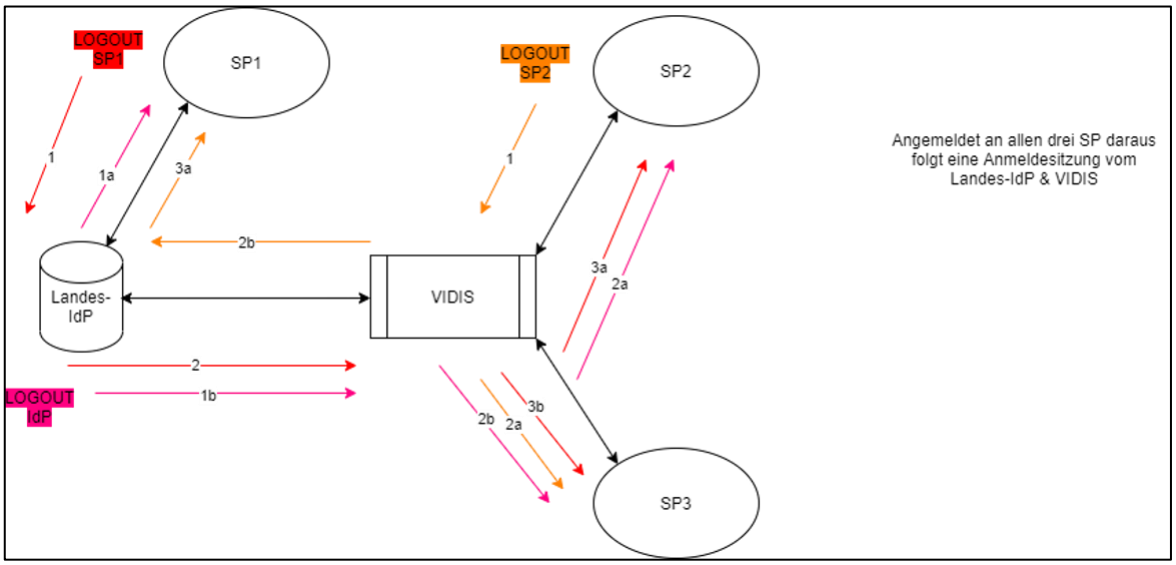
Log-out

Die Pilotländern haben die Anforderung nach einem „Log-out from all Services and Devices“ formuliert. Der Single Log-out ist zunächst optional, soll aber schrittweise umgesetzt werden. Insbesondere aufgrund einer Vielzahl geteilter Endgeräte an Schulen ist eine Abmeldung an allen Diensten erforderlich. Dies entspricht der höchsten Sicherheitsstufe um die Übernahme von Anmeldesitzungen (auch versehentlich) zu verhindern. Folgendes Schaubild stellt die Prozesse des Log-out dar.

Das Verhalten des Landes-IdP steht immer unter der Hoheit des Landes. Das bedeutet, dass VIDIS im Zweifelsfall die Log-out-Informationen weiterleitet und der Landes-IdP selbständig entscheidet, ob auch seine eigene Anmeldesitzung ungültig gemacht wird und gegebenenfalls andere Systeme informiert werden.

Ein Logout am Serviceprovider führt dazu, dass Benutzer:innen am Dienst ausgeloggt werden und ein Logout-Aufruf am VIDIS-System erfolgt.

Das VIDIS-System invalidiert anschließend die Session und leitet diese Information an das Landessystem (IdP) und alle weiteren angeschlossenen Serviceprovider weiter.



Aufbau

- Fünf Systeme (schwarze Formen)
    a. Landessystem (Landes-IdP)
    b. VIDIS-System (VIDIS)
    c. Digitales Bildungsangebot 1 (SP1)
    d. Digitales Bildungsangebot 2 (SP2)
    e. Digitales Bildungsangebot 3 (SP3)
- Vier konfigurierte SSO-Anbindungen (schwarze Pfeile)
    a. Landessystem (Landes-IdP) ↔ Digitales Bildungsangebot 1 (SP1)
    b. Landessystem (Landes-IdP) ↔ VIDIS-System (VIDIS)
    c. VIDIS-System (VIDIS) ↔ Digitales Bildungsangebot 2 (SP2)
    d. VIDIS-System (VIDIS) ↔ Digitales Bildungsangebot 3 (SP3)

Ausgang

- Benutzer:in ist an allen Systemen angemeldet
- Landessystem (Landes-IdP)
- VIDIS-System (VIDIS)

- Digitales Bildungsangebot 1 (SP1)
- Digitales Bildungsangebot 2 (SP2)
- Digitales Bildungsangebot 3 (SP3)
- Benutzer:in besitzt zwei SSO-Anmeldesitzungen
    - Anmeldesitzung 1
        - Landessystem (Landes-IdP) ↔ Digitales Bildungsangebot 1 (SP1)
        - Landessystem (Landes-IdP) ↔ VIDIS-System (VIDIS)
    - Anmeldesitzung 2
        - VIDIS-System (VIDIS) ↔ Digitales Bildungsangebot 2 (SP2)
        - VIDIS-System (VIDIS) ↔ Digitales Bildungsangebot 3 (SP3)

Szenario 1 Logout SP1 (rot) - SP-initiated
1 - Logout erfolgt an digitalem Bildungsangebot 1 (SP1) und wird an Landes-IdP weitergeleitet.

2 - Landes-IdP invalidiert Anmeldesitzung und leitet Abmeldung im Backchannel an VIDIS-System (VIDIS) weiter.

3a - VIDIS-System invalidiert Anmeldesitzung und leitet Abmeldung im Backchannel an das digitales Bildungsangebot 2 (SP2) weiter.

3b - Analog leitet das VIDIS-System die Abmeldung im Backchannel an das digitales Bildungsangebot 3 (SP3) weiter.

Szenario 2 Logout SP2 (orange) - SP-initiated
1 - Logout erfolgt an digitalem Bildungsangebot 2 (SP2) und wird an das VIDIS-System (VIDIS) weitergeleitet.

2a - VIDIS-System invalidiert Anmeldesitzung und leitet Abmeldung im Backchannel an das digitale Bildungsangebot 3 (SP3) weiter.

2b - Analog leitet das VIDIS-System die Abmeldung im Backchannel an den Landes-IdP weiter.

3a - Landes-IdP invalidiert Anmeldesitzung und leitet Abmeldung im Backchannel an das digitale Bildungsangebot 1 (SP1) weiter.

Szenario 3 Logout IdP (rosa) - IdP-initiated
1a - Logout erfolgt an Landes-IdP, Anmeldesitzung wird invalidiert und die Abmeldung im Backchannel an das digitale Bildungsangebot 1 (SP1) weitergeleitet.

1b - Analog leitet der Landes-IdP die Abmeldung im Backchannel an das VIDIS-System (VIDIS) weiter.

2a - VIDIS-System invalidiert Anmeldesitzung und leitet Abmeldung im Backchannel an das digitales Bildungsangebot 2 (SP2) weiter.

2b - Analog leitet das VIDIS-System die Abmeldung im Backchannel an das digitales Bildungsangebot 3 (SP3) weiter.

Sicherheitsaspekte

Wie wird die Security im VIDIS-Dienst umgesetzt

Die Aktivierung der Security-Header erfolgt über die Konfiguration des Webservers, z.B. durch eine .htaccess Datei. Ein minimalistisches Beispiel für die .htaccess sieht z.B. so aus:

```
# Extra Security Headers
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
Header always append X-Frame-Options SAMEORIGIN
Header set X-Content-Type-Options nosniff
Header set Strict-Transport-Security max-age=17280000
Header set Referrer-Policy no-referrer
Header set Feature-Policy "camera 'none'; microphone 'none'; geolocation 'none'; payment 'none';"
Header set Content-Security-Policy "default-src 'self';"
</IfModule>
```

3rd Party Libs

Alle verwendeten Bibliotheken auf Code Ebene werden von uns auf Schadsoftware geprüft und getestet bevor wir Sie in VIDIS integrieren.

Tokens und Cookies

Es werden keinerlei Userinformationen über Tokens und Cookies versendet bzw. gespeichert. Alle verwendeten Tokens werden in Abschnitt 4 aufgelistet. Die verwendeten Cookies sind für die Funktionalität von VIDIS zwingend erforderlich. Es handelt sich hierbei lediglich um First-Party-Cookies.

SSL-Verschlüsselung

Standardmäßig verschlüsselt der VIDIS-Dienst alle internen und externen Netzwerkverbindungen per SSL. Bei einer sogenannten „SSL-Verschlüsselung" (Secure Sockets Layer) wird die Verbindung zwischen einem Server und einem Client verschlüsselt.
Sie kann somit nicht von Dritten eingesehen werden. Die Verschlüsselung erfolgt in der Regel über das Protokoll https.

X-Frame-Options

SAMEORIGIN

Standardmäßig ist die Option SAMEORIGIN für das VIDIS-IAM und den VIDIS-Testdienst gesetzt. Diese Einstellung bewirkt, dass nur von vidis.schule und deren Subdomains das Einbinden via Frame möglich ist. Es ist ein Aufruf nur per https:// möglich. Versucht eine fremde Domain die Inhalte von VIDIS einzubinden, blockiert der Browser die Anzeige der Inhalte.

Response Header

X-XSS-Protection

Aktiviert eine generische Funktion zur Unterdrückung von sog. Reflective Cross-Site-Scripting Attacken. Bei diesem Angriffstyp wird JavaScript- oder HTML-Code, der über die URL oder POST-Parameter an die Seite übergeben werden wieder an die Benutzer:innen ausgegeben, also

“reflektiert”. Bei einer solchen Lücke lassen sich dann z.B. Links konstruieren, die bösartiges JavaScript im Browser der Benutzer:innen ausführen.

Die XSS-Protection der Browser unterdrückt genau das.

Content Security Policy

VIDIS setzt alles was möglich ist bestmöglich um, es gibt aber auch notwendige Einstellungen um den Dienst nutzen zu können wie z.B. **unsafe-inline** für **script-src** und **style-src** die zugelassen werden müssen, da dies für die Funktionalität zwingend erforderlich ist.

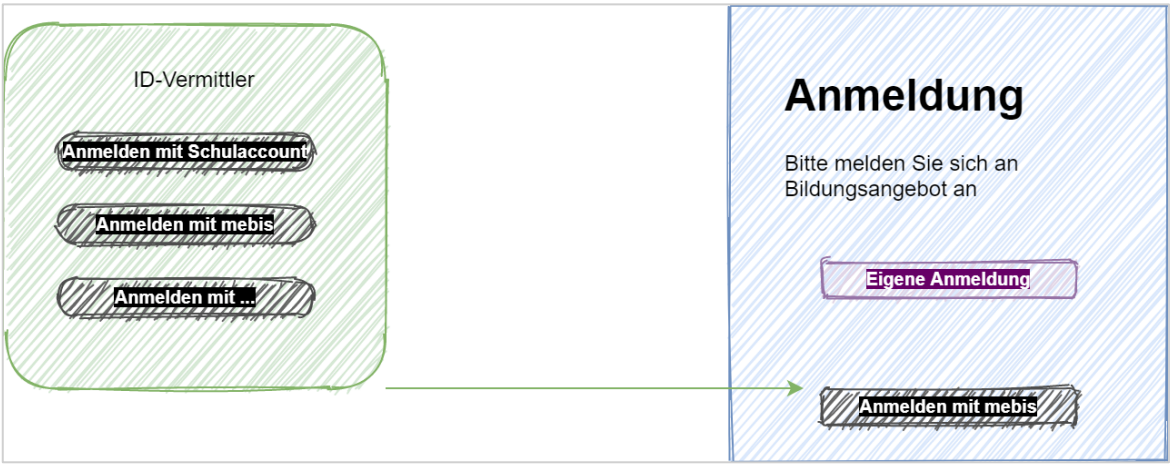
Anbindung und Integration

Öffentlicher Endpunkt

Der öffentliche OpenID-Connect (OIDC) Konfigurations-Endpunkt des PoC befindet sich unter folgender Adresse: https://aai.vidis.schule/auth/realms/vidis/.well-known/openid-configuration

Integration VIDIS Button

VIDIS bietet eine (JavaScript) Client-Bibliothek an, die von Bildungsangeboten eingebunden werden kann. Sie hat zum Ziel, die Usability deutlich zu verbessern, ohne zu stark in das Userinterface der Bildungsangebote einzugreifen. Eine Teilnahme an VIDIS ist auch ohne diese Client-Bibliothek möglich. Allerdings ist es wünschenswert den Button einzubinden.



Code zur Einbindung auf Anmeldeseite

Tokens und Parameter

Welche Daten werden übermittelt?

access_token: Ein access_token ist ein Artefakt , das vom Auth-Server bereitgestellt wird und einer Anwendung den Zugriff auf eine Ressource ermöglicht.

refresh_token: Ein refresh_token ist ist ein Artefakt mit Anmeldeinformationen, mit dem eine Clientanwendung neue Zugriffstoken erhält, ohne dass die Benutzer:innen erneut aufgefordert werden muss, sich anzumelden.

scope: Der Scope beschreibt die Berechtigungen, die ein:e Benutzer:in besitzt.

expires_in: Die Lebensdauer des access_token wird durch die SSO-Sitzungsleerlaufeinstellung gesteuert. Beispiel: 30 Minuten = 30 * 60 = 1800 Sekunden (der Wert expires_in)

refresh_expires_in: Die Lebensdauer des refresh_token wird durch die SSO-Sitzungsleerlaufeinstellung gesteuert. Beispiel: 30 Minuten = 30 * 60 = 1800 Sekunden (der Wert refresh_expires_in)

token_type: token_type ist ein Parameter im Aufruf zum Generieren von Access Token an den Autorisierungsserver, der im Wesentlichen darstellt, wie ein access_token generiert und für Ressourcenzugriffsaufrufe präsentiert wird. Diese Zugriffe geben token_type im Aufruf zur Generierung des Zugriffstokens an einen Autorisierungsserver an.

not-before-policy: Durch das Pushen dieser Richtlinie wird sichergestellt, dass alle Token, die vor diesem Zeitpunkt ausgestellt wurden, ungültig werden.

session_state: Der Sitzungsstatus ermöglicht, Variablen zwischen erneuten Aufrufen für die Usersitzung freizugeben.

Mit verschiedenen Tools lassen sich die Werte der Tokens in dem man Sie decodiert auslesen. Dort sieht man welche Informationen in den Tokens stehen.

Anlage 2:

Spezifikation zu Schnittstellen (Diensteanbieter)

Informationen für Service Provider (SP)

Um die geordnete Anbindung eines "Service Providers" an das VIDIS-System zu ermöglichen, müssen entsprechende Metadaten gemäß https://openid.net/specs/openid-connect-discovery-1_0.html ausgetauscht werden.

In diesem Dokument wird ausschließlich auf den Fall einer Anbindung von Angeboten (Webseiten und Apps) als OpenID Connect Client eingegangen.

Es werden in späteren Projektphasen noch weitere SSO-Technologien für den Einsatz evaluiert. Es ist jedoch unwahrscheinlich, dass der produktive VIDIS-Dienst später viele weitere SSO-Technologien unterstützen wird.

Pilotsystem

Ein Demosystem / Proof of Concept (PoC) ist derzeit in Betrieb. Alle Tests, insbesondere die Test-Anbindungen, werden derzeit an diesem VIDIS-System durchgeführt. Dieses Demosystem wird in Zukunft dauerhaft als Integrations- und Testsystem für die VIDIS-Infrastruktur dienen und eine Anbindung wird Voraussetzung für die Anbindung an das Pilotsystem sein. Das Pilotsystem verhält sich analog und die Inbetriebnahme des Pilotsystems läuft aktuell.

Anbindung eines OpenID Connect Client

Für die Anbindung eines OpenID Connect Clients müssen folgende Parameter ausgetauscht und sowohl im VIDIS-System als auch beim anzubindenden OpenID Connect Client konfiguriert werden.

FWU/VIDIS an SP zusammengefasst

- **"ClientID":** der Identifikator des anzubindenden OpenID Connect Clients
- **"Client Secret"**: ein zwischen VIDIS und dem OpenID Connect Client geteiltes Geheimnis
- **"Authorize Endpoint":** https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/auth
- **"Access Token Endpoint":** https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/token
- **"end_session_endpoint"** https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/logout

Die maschinenlesbare OpenID Connect Konfiguration befindet sich zusammengefasst unter: https://aai.vidis.schule/auth/realms/vidis/.well-known/openid-configuration

SP an FWU/VIDIS zusammengefasst

Notwendig:

- **"Valid Redirect URIs":** zulässige Redirect URIs
- **"BaseURL":** zum Testen der Verbindung von FWU-Seite (Das ist der Einstiegspunkt bzw. das Login Formular)
- **"Deeplink" ins Angebot:** Wird benötigt, um von Landesportalen mit Session direkt in Ihr Angebot zu springen ohne erneute Anmeldung. Dafür muss ein Parameter angehängt werden → "kc_idp_hint" (siehe unten: Weitere technische Voraussetzungen)

Optional:

- **"Backchannel-Logout-URL":** zulässige Logout-URL
- Social-Media-Vorschaubild für Deeplink: Hilfreich bei Verlinkung bzw. Anzeige in Lern-Management-Systemen, Mediatheken und Portalen

Beschreibung OIDC-Claims

Bezeichnung	OIDC-Name	Wert(e)	
Eineindeutige ID (Sub, ggf. Pseudonym, ID-Token)	sub	HMAC-512	Garantiert

Integration VIDIS-Login

Was ist der VIDIS-Login?

Das Ziel des VIDIS-Logins ist es, jedem Schüler und Lehrer ein einziges Konto zur Verfügung zu stellen, mit dem man sich überall einloggen kann.

Dazu wird eine bestehende Schul-Login als IDP verwendet. Das bedeutet, dass der VIDIS-Login die Benutzer:innen in das IDP-System einloggt, das die Schule verwendet und zu Ihnen zurückkehrt.

Die Benutzer:innen müssen also die IDP auswählen, die er verwenden kann, was beispielsweise auch über den VIDIS-Button geschehen kann.

Sie können die Funktionalität hier testen: https://tp.fwu.intension.eu/?version=latest

Voraussetzungen für die Integration des VIDIS-Login:

- Unterstützung OpenID-Connect

Integration des Vidis Login Buttons:

Allgemeine Vorgehensweise:

2. Hinzufügen eines CDN-Links
3. Bauen Sie die Webkomponente des Vidis Login-Buttons ein
4. Geben Sie dem Button Ihren Login-Link
5. Konfiguration des Vidis Login-Buttons
    - Größe (size)
    - Cookie (cookie)

1. Hinzufügen eines CDN-Links

Damit der Vidis Login Button funktioniert, müssen Sie einen CDN-Link in Ihre Website einbinden:

```
<script src="https://repo.vidis.schule/repository/vidis-cdn/latest/vidisLogin.umd.js"></script>
```

Der Link, den Sie normalerweise verwenden würden,
lautet: https://repo.vidis.schule/repository/vidis-cdn/latest/vidisLogin.umd.js

Wenn Sie eine bestimmte Version bevorzugen: https://repo.vidis.schule/repository/vidis-cdn/{version}/vidisLogin.umd.js

Zum Beispiel: https://repo.vidis.schule/repository/vidis-cdn/0.11.0/vidisLogin.umd.js

2. Bauen Sie die Webkomponente des Vidis Login-Buttons ein

Wenn Sie sich entschieden haben, wo der Vidis-Login-Button platziert werden soll, können Sie ihn wie folgt hinzufügen:

```
<vidis-login loginurl=""></vidis-login>
```

3. Geben Sie den Login-Link für den Button an

WICHTIG: Sie müssen die Loginurl Ihres Systems angeben, sonst kann der Button nicht funktionieren.

WICHTIG: Die Loginurl muss mit "https://" beginnen, um erkannt zu werden.

Die Benutzer:innen umgeleitet, indem die angegebene Loginurl mit diesem Abfrageparameter ergänzt wird: kc_idp_hint

4. Konfiguration des Vidis Login Buttons

Sie können den Vidis Login Button mit den folgenden Attributen anpassen:

7. Größe: Bestimmt die Größe des Buttons.
    b. Werte:

i. "L": Groß, zeigt die Schaltfläche in einer großen Version an. Dies ist auch die Standardeinstellung.

ii. "M": Mittel, zeigt die Schaltfläche in einer mittleren Version an.

iii. "S": Klein, zeigt die Schaltfläche in einer kleinen Version an.

c. Cookie: Aktiviert oder deaktiviert die Speicherung der letzten Auswahl der Benutzer:innen in einem Cookie.

i. Es wird empfohlen, diese Option zunächst auf "false" zu setzen und erst dann zu aktivieren, wenn Benutzer:innen den Cookies auf der Website zugestimmt hat, um rechtliche Probleme zu vermeiden.

Ein vollständiges Beispiel:

Vidis-Login Example

```
<script src="https://repo.vidis.schule/repository/vidis-cdn/1.0.1/vidisLogin.umd.js"></script>
...
<vidis-login loginurl="https://www.domain.de/path-to-auth/" size="L" cookie="true"></vidis-login>
```

Kompatibilität:

Der Vidis Login Button ist als Webkomponente erstellt und sollte daher in jeder html-basierten Umgebung funktionieren, insbesondere in jedem SPI-Framework wie Vue, Angular und React.

Technisch gesehen, wenn man weiß, wie man eine Webkomponente in andere Apps (wie Android oder IOS) integriert, sollte der Button auch out of the box funktionieren, ist aber noch nicht dafür getestet.

Weitere technische Voraussetzungen

Automatische Registrierung bei initialer Anmeldung

Voraussetzung für Service Provider ist, dass Benutzer:innen, die sich an dem digitalen Bildungsangebot erstmalig anmelden, bei der Anmeldung automatisch registriert werden.

Weitergabe des Parameter kc_idp_hint

Voraussetzung für Service Provider ist, die automatische Weitergabe des Parameter kc_idp_hint (z.B. "?kc_idp_hint=Landessystem") während der Anmeldung. Für einige Anwendungsfälle (z.B. Direktaufruf aus Landessystemen heraus) ist die Vorauswahl eines Landes-IdP wichtig. Der VIDIS-Dienst unterstützt diese Vorauswahl durch Übergabe des Parameter kc_idp_hint. Dieser Parameter muss also bei aufrufen (z.B. bei Authorization Requests) uneditiert weitergegeben werden und darf nicht herausgefiltert werden.

Userinfo überprüfen

Über den endpoint https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/userinfo können Sie sich die Übermittelten Userdaten unsererseits ansehen.

Das funktioniert wie folgt.

Schritt 1: Zuerst muss ein Token generiert werden.

Dieser Token (access_token) fungiert als "Bearer Token" der zum Abruf der Userinfo genutzt werden kann und zu Debugging zwecken, der Redirect Flow wird bei der finalen Integration verwendet.

```
curl --location --request POST 'https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'username=XXXXX' \
--data-urlencode 'password=XXXXX' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'client_id=account'
```

Schritt 2: Jetzt lassen sich die Userdaten mit dem Token abrufen

```
curl --location --request GET 'https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/userinfo' \
--header 'Authorization: Bearer <TOKEN>
```

oder alternative zu Schritt 2 wäre es den JWT Token zu dekodieren, um die Userdaten auslesen zu können. Hierzu kann beispielsweise auch ein entsprechendes Online Tool verwendet werden (z. B. über https://devtoolzone.com/decoder/jwt, https://jwt.io/ etc.), sofern es sich nicht um reale Userdaten handelt.

Das Ergebnis ist ein JSON mit den Userdaten:


```
{
  "sub": "39e0063a-8377-4a1c-bd15-ea16f65a5a15",
}
```


Fragen & Anregungen

Für Fragen und Anregungen melden Sie sich gerne jederzeit unter vidis@fwu.de

ANLAGE 3:

Spezifikationen zu den Datensätzen

Datenmodell:
In der Pilotphase werden die folgenden benötigten Daten verarbeitet

	Lehrkraft & Schüler/in (innerhalb SSO-Session)									
	ID (IdP) → Pseudony-misierung (VIDIS)→ Pseudonym (SP)	**Akronym**	**Land**	**Heimat-organisation**	**Rolle (Unterschied Lehrkraft/ Schüler/in)**	**Schul-identifikator (Stamm-schule)**	**E-Mail (Pflichtfeld im Standard, je nach technischen Voraussetzungen)**	**Name/ Vorname**	**Akronym**	**Lizenzen**
Pilotphase Teil 1 (ab Q2'22)	✓	keine Erhebung /Verarbeitung	keine Erhebung/ Verarbeitung	keine Erhebung/Verarbeitung	✓*	keine Erhebung/ Verarbeitung	Dummy/Leer	keine Erhebung/ Verarbeitung	keine Erhebung/ Verarbeitung	keine Erhebung/ Verarbeitung
Pilotphase Teil 1,5 (ab Q3'22)	✓	keine Erhebung /Verarbeitung	keine Erhebung/ Verarbeitung	keine Erhebung/Verarbeitung	✓**	keine Erhebung/ Verarbeitung	Dummy/Leer	keine Erhebung/ Verarbeitung	keine Erhebung/ Verarbeitung	keine Erhebung/ Verarbeitung
Pilotphase Teil 2 (ab ca. Q4'22 geplant) "Kern-Datensatz"	✓	keine Erhebung /Verarbeitung	keine Erhebung/ Verarbeitung	keine Erhebung/ Verarbeitung	✓**	✓**	Dummy/Leer	Dummy /Leer	Dummy /Leer	keine Erhebung/ Verarbeitung
Pilotphase Teil 3 (ab Q3'23) "erweiterter Kerndatensatz"	✓	✓	✓	✓	✓**	✓**	Emailadresse IdP oder pseudonymisiert von VIDIS**	✓** nur Lehrkräfte	✓** nur Schüler	Wird aktuell nicht umgesetzt

*
nur Lehrkräfte nehmen an Pilotphase teil
** Nachweis der Notwendigkeit zur Verarbeitung jedes Attributs muss vom Anbieter des Angebots erbracht werden.

3 Vom Diensteanbieter festzulegende Verwendungszwecke gem. 6.3. f des Pilotvertrags Diensteanbieter 4 * Verwendungszwecke und deren Begründung können auf einem gesonderten Blatt erfolgen; die vom Diensteanbieter festzulegenden Verwendungszwecke dürfen nicht der Zweckbindung aus 6.3. a entgegenstehen.					
	Rolle (Lehrkraft/ Schüler/in)	**Schulidentifikator (Stammschule)**	**E-Mail-Adresse**	**Name, Vorname der Lehrkraft**	**Akronym der/s Schülers/in**
ja/nein					
Verwendungszweck(e) und deren Begründung*					

VIDIS

Brandbook

V2 19.01.2022

Verantwortlich

FWU Institut für Film und Bild
in Wissenschaft und Unterricht
gemeinnützige GmbH

Content

Januar 2022

VIDIS ist eine sichere Plattform, die Schulen ermöglicht ihren Weg in die digitale Welt zu finden.

The enabler

Wir vermitteln digitale Identitäten in Schulen.

Wir bringen sichere, länderübergreifende, einheitliche Standards und kontrollierten Datenfluss.

Unsere Mission: sichere und digitale Bildungsinfrastruktur für Deutschland

Einfach.
Sicher.
Neutral.
Integrativ.

Unsere Prinzipien sind ein Leitfaden dafür, wie sich die Marke VIDIS anfühlt.

Es ist wichtig, sie bei jeder Kommunikation mit unserer Zielgruppe oder bei der Entwicklung einer neuen Service, Dienstleistung oder eines Produkts zu berücksichtigen.

Vidis vereinfacht den Zugang zu Wissen. Verschiedene Portale aller Bundesländer macht Vidis mit einem einfach Login zugänglich. Es ist ein geschützter Ort. Vidis ist neutral und hat und bringt den Überblick.

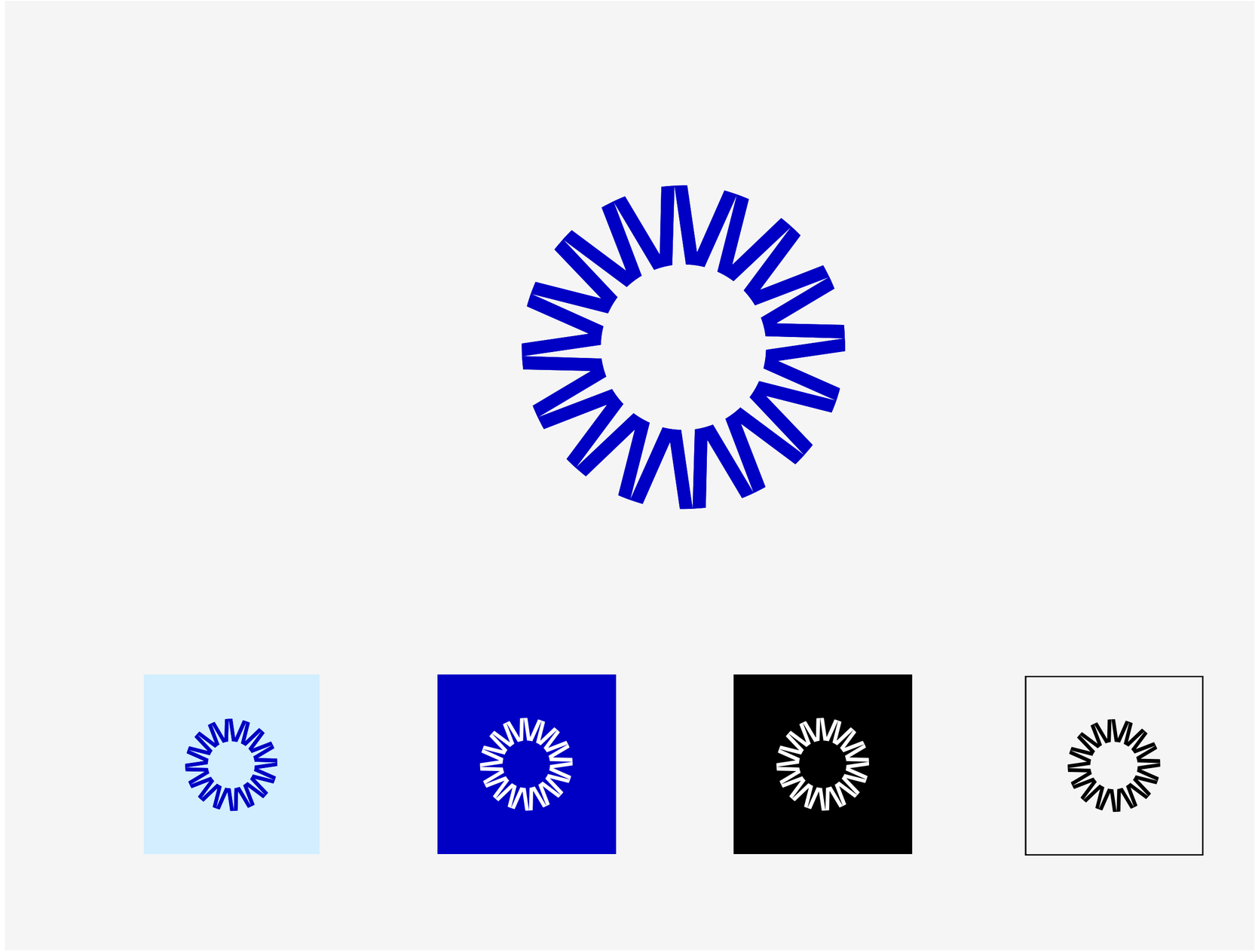
Logo Wort-Bild-Marke

Das Signet symbolisiert den Zugang zu den Lernplattformen der 16 Bundesländer. Gleichzeitig hat es eine Assoziation mit einem Auge oder einer Pupille und spielt damit auf die lateinische Übersetzung von Vidis (“du hast gesehen”) an.

Die Wortmarke ist sehr schlicht, einfach und gut lesbar gestaltet. So simple wie der Service den VIDIS anbietet.

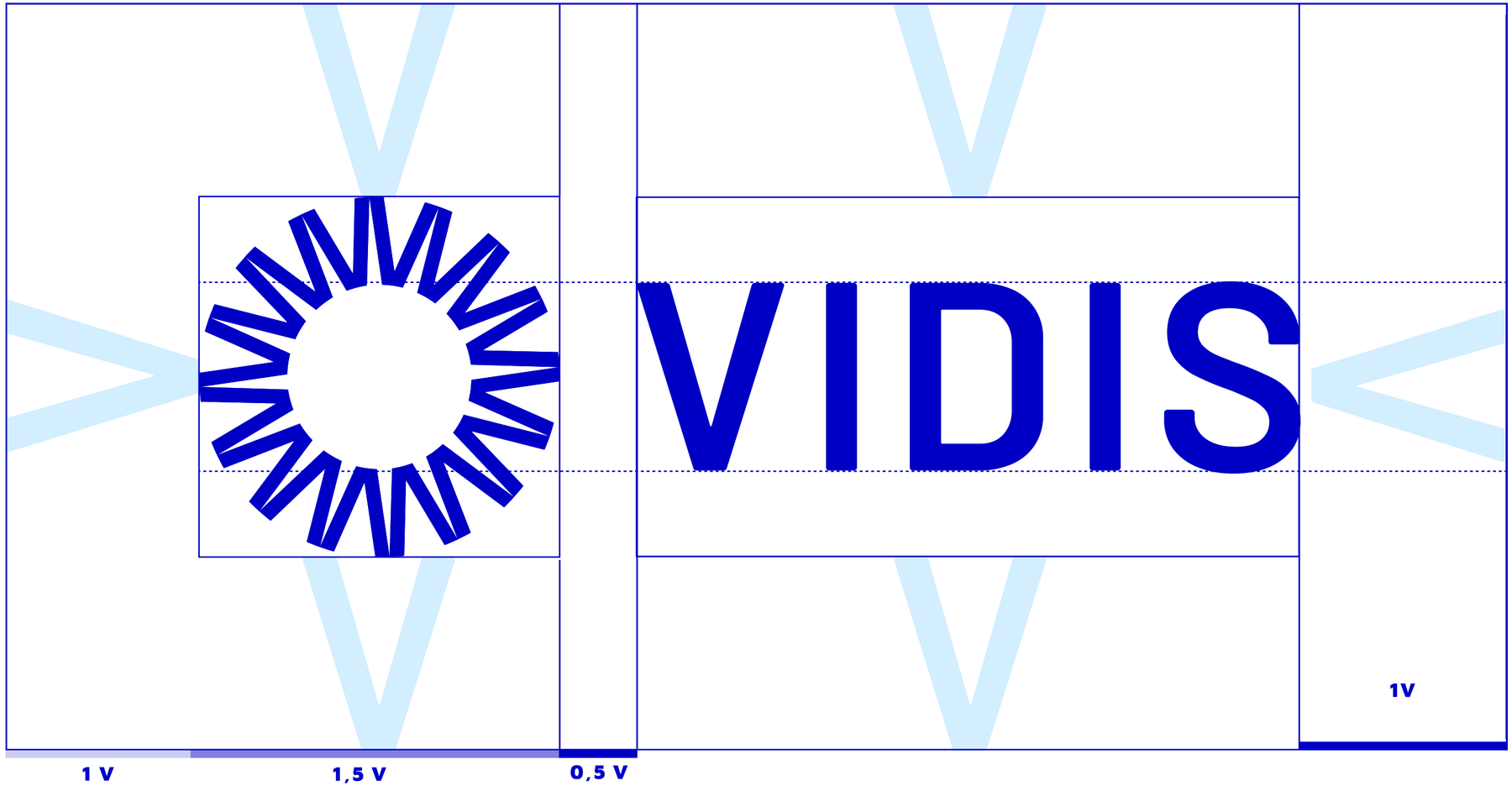
Logo Bildmarke

Das Signet symbolisiert die 16 Bundesländer mit jeweils einem “V”. Die wiederum einen Kreis formen. Gemeinsam bilden sie also einen geschützen und sicheren Raum. Es steht symbolisch für den sicheren Zugang zu allen Lernplattformen der 16 Ländern.



Logo Schutzzone

Die Wortbildmarke wird geschützt durch eine klar definierte Schutzzone, die oben, unten, rechts und links des Logos je die Höhe eines “V” beträgt.



140 px

Do`s

Das Logo kann auf blauen, schwarzen und grauen Untergrund stehen.

Ebenso kann das Logo auf weiß in blau, schwarz und grau stehen.

Auch helle und ruhige Fotohintergünde sind erlaubt.

Dont`s

Vidis Länderlogos

Das Vidis Logo kann in Kombination mit den Ländern gesetzt werden.
Ein Strich teilt das Vidis Logo dann vom entsprechenden Länderwappen oder auch dem Schriftzug des jeweiligen Bundeslands.

VIDIS | Bayern

VIDIS

VIDIS

Vidis Button

VIDIS Login

Anmeldung mit Schulaccount

Anmeldung
Bayern Cloud Schule

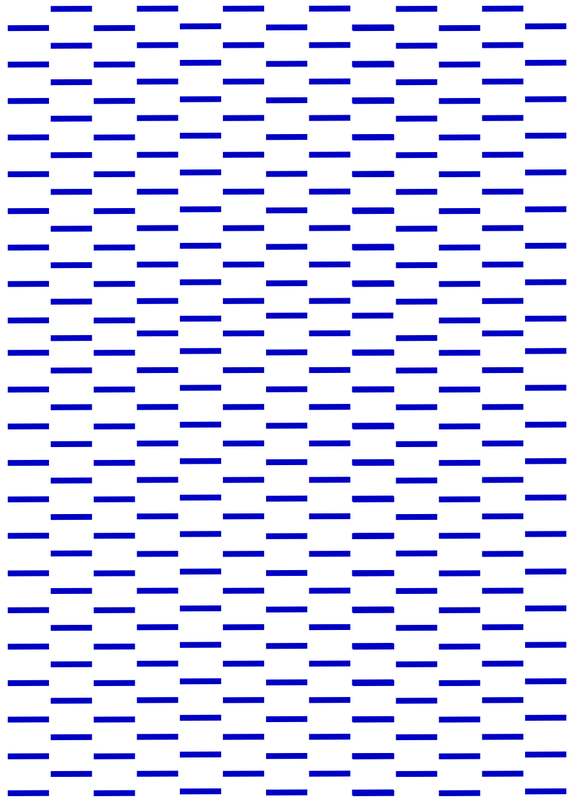
Anmeldung
Bayern Cloud Schule

Anmeldung
Bayern Cloud Schule

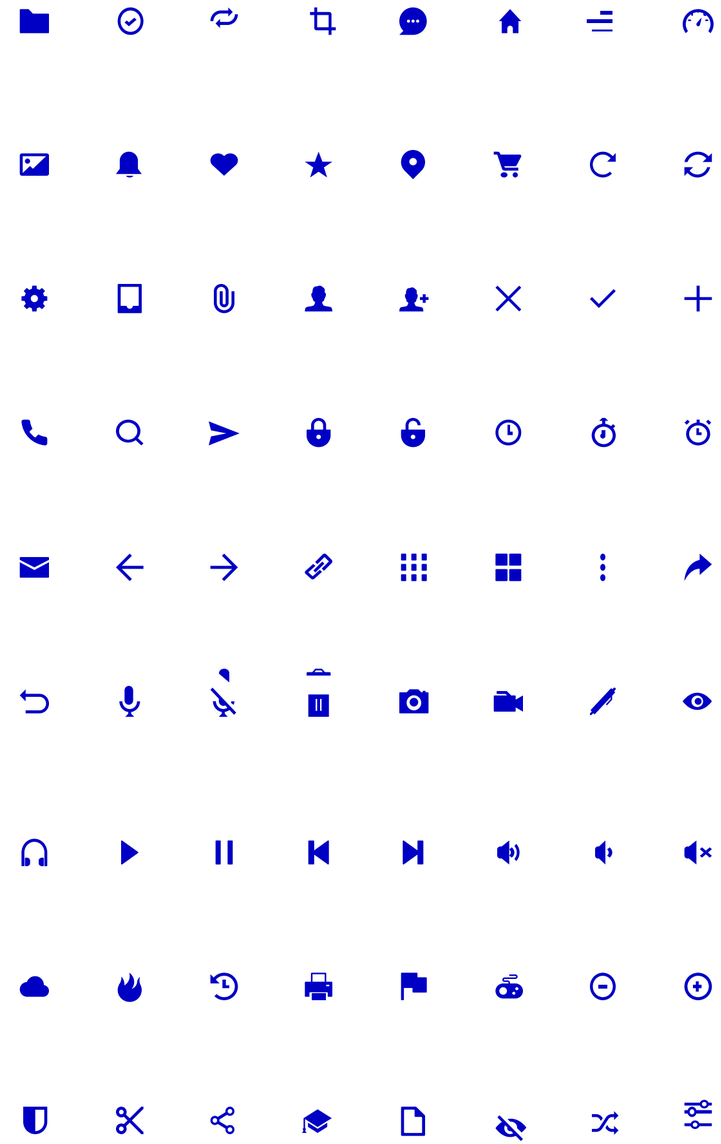
VIDIS | Bayern

VIDIS

PATTERN



ICONS



Barlow

ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

1234567890%6/()

ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

1234567890%6/()

H1

Unsere Vision: Einfach und sicher.

H2

Wir bringen sichere, länderübergreifende, einheitliche Standards und kontrollierten Datenfluss.

H3

DER VERMITTLUNGSDIENST VIDIS

H4

Wir vermitteln digitale Identitäten in Schulen.

COPY

Zusammenarbeit zwischen den Identitätsanbietern und den Diensteanbietern, schafft damit den Zugang zu den Dienstleistungen, setzt Standards, stellt Regeln und Normen auf und beschreibt und steuert Prozesse.

Typografie

Style	Größe	Zeilenhöhe	Spationierung
Barlow Bold	72	110%	0%
Barlow Bold	32	130%	0%
Barlow Bold	16	130%	15%
Barlow Regular	72	120%	0%
Barlow Regular	32	130%	0%
Barlow Regular	24	140%	0%
Barlow Regular	16	140%	0%
Barlow Regular	12	140%	0%
Barlow Regular	9	145%	5%

Farbe - Primary

Hex: #0000C4

RGB: 0/0/196

CMYK: 100/100/0/23

Hex: #99D7FF

RGB: 153/215/255

CMYK: 40/16/0/0

Hex: #FFFFFF

RGB: 255/255/255

CMYK: 0/0/0/0

Farbe - Primary Schattierungen

#0000C4	#0032C4	#0064C4	#1B8FD9	#99D7FF	#B2E1FF	#E5F5FF
RGB: 0/0/196	RGB: 0/50/196	RGB: 0/100/196	RGB: 27/143/217	RGB: 153/215/255	RGB: 178/225/255	RGB: 229/245/255
CMYK: 100/100/0/23	CMYK: 100/74/0/23	CMYK: 100/49/0/23	CMYK: 88/34/0/15	CMYK: 40/16/0/0	CMYK: 30/12/0/0	CMYK: 10/4/0/0

Farbe - Secondary Schattierung

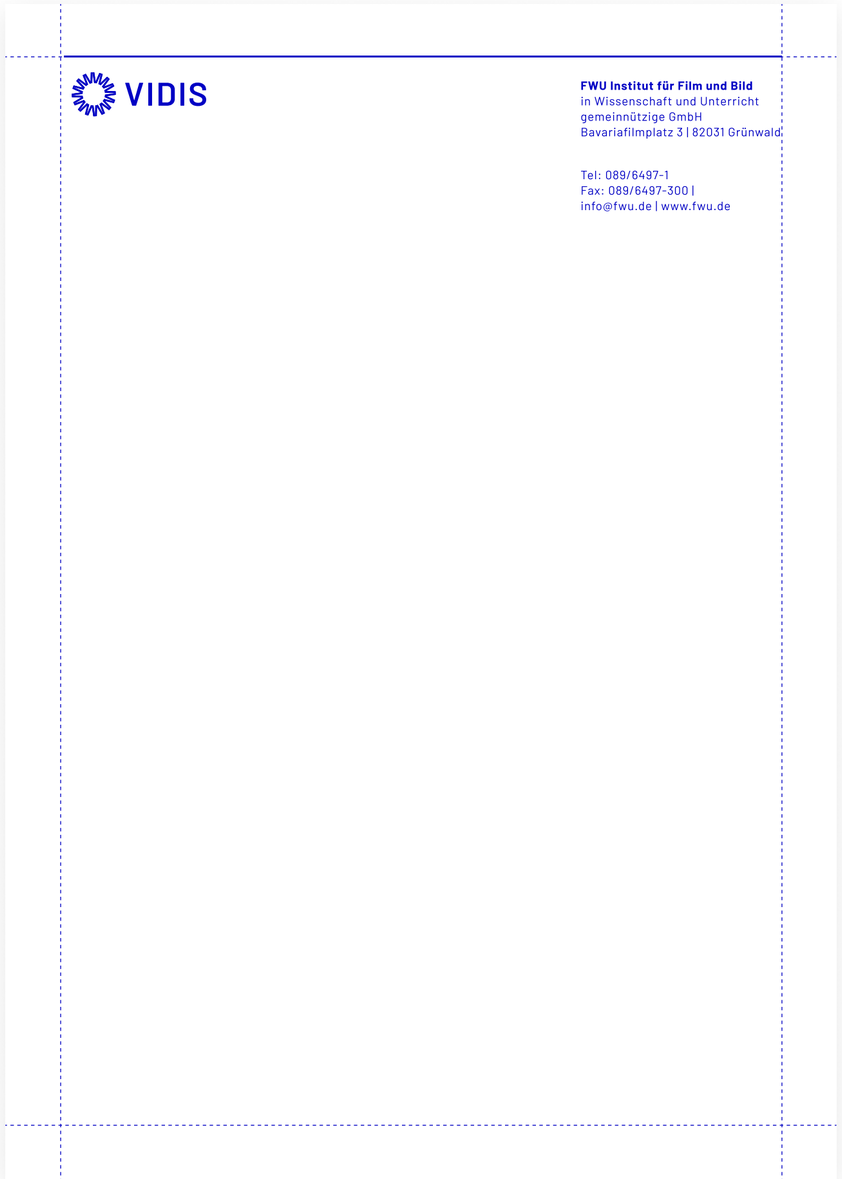
Hex: #F1943F	Hex: #F39D4E	Hex: #F9AA62	Hex: #FBC87B	Hex: #F9DB9F	Hex: #FCEDCF	Hex: #FEF9EF
RGB: 29/86/60	RGB: 29/86/60	RGB: 29/92/68	RGB: 36/94/73	RGB: 29/86/60	RGB: 29/86/60	RGB: 29/86/60
CMYK: 0/39/74/5	CMYK: 0/35/68/5	CMYK: 0/32/61/2	CMYK: 0/20/51/2	CMYK: 0/12/36/2	CMYK: 0/6/18/1	CMYK: 0/2/6/0

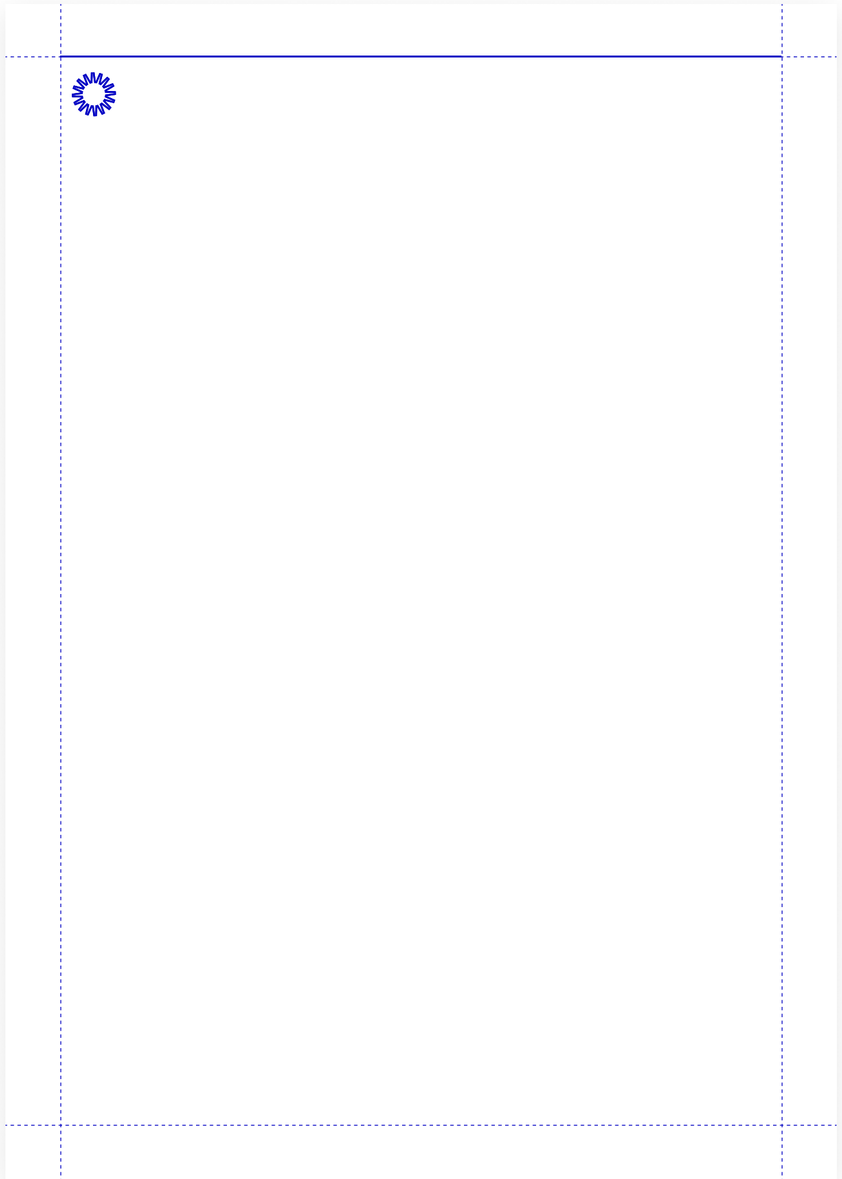
Hex: #000000	Hex: #000000	Hex: #333333	Hex: #666666	Hex: #999999	Hex: #CCCCCC	Hex: #E5E5E5
RGB: 0/0/0	RGB: 0/0/0	RGB: 51/51/51	RGB: 102/102/102	RGB: 153/153/153	RGB: 204/204/204	RGB: 229/229/229
CMYK: 0/0/0/100	CMYK: 0/0/0/100	CMYK: 0/0/0/80	CMYK: 0/0/0/60	CMYK: 0/0/0/40	CMYK: 0/0/0/20	CMYK: 0/0/0/10

Homepage


VIDIS
ID Plattform
für sichere Bildung
Zugang Anfragen
Home
Über uns
Services
Kontakt
Log in
Registrieren
Einfach und sicher.
Eine Initiative von
MacBook Pro

Briefpapier





Visitenkarten

VIDIS

FWU Institut für Film und Bild
in Wissenschaft und Unterricht
gemeinnützige GmbH

Bavariafilmplatz 3
D 82031 Grünwald

Andreas Koschinsky

Leiter Mediendienste

Tel: +49(0)89 6497 249
anke.baecker@fwu.de

VIDIS

FWU Institut für Film und Bild
in Wissenschaft und Unterricht
gemeinnützige GmbH

Bavariafilmplatz 3
D 82031 Grünwald

Michael Frost

Geschäftsführer

Tel: +49(0)89 6497 249
anke.baecker@fwu.de

Werbemittel

VIDIS

ID PLattform
für sichere Bildung

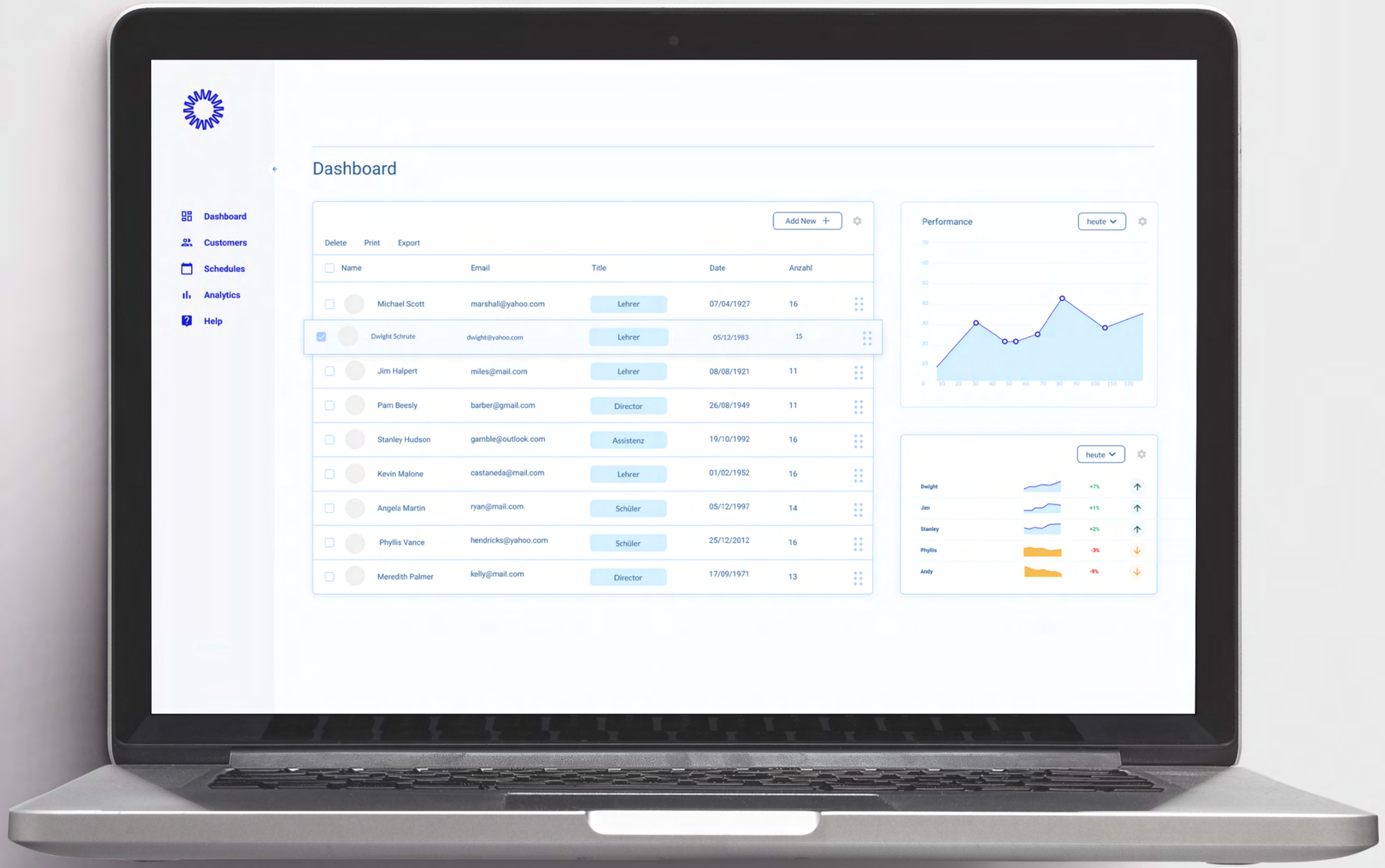
Einfach
und sicher.

**“VIDIS” steht für
“Vermittlungsdienst für das digitale
Identitätsmanagement in Schulen“.**

Damit ist der Vermittlungsdienst die operative Schaltstelle zwischen den Identitätsanbietern (Identity Provider, IdP) und den Dienstanbietern (Service Provider, SP). Er regelt die Zusammenarbeit zwischen den Identitätsanbietern und den Diensteanbietern, schafft damit den Zugang zu den Dienstleistungen, setzt Standards, stellt Regeln und Normen auf, beschreibt und steuert Prozesse, sorgt für eine reibungslose Ab- und Anmeldung bzw.Akkreditierung, damit beide Seiten die Dienste nutzen können.

Eine Initiative von

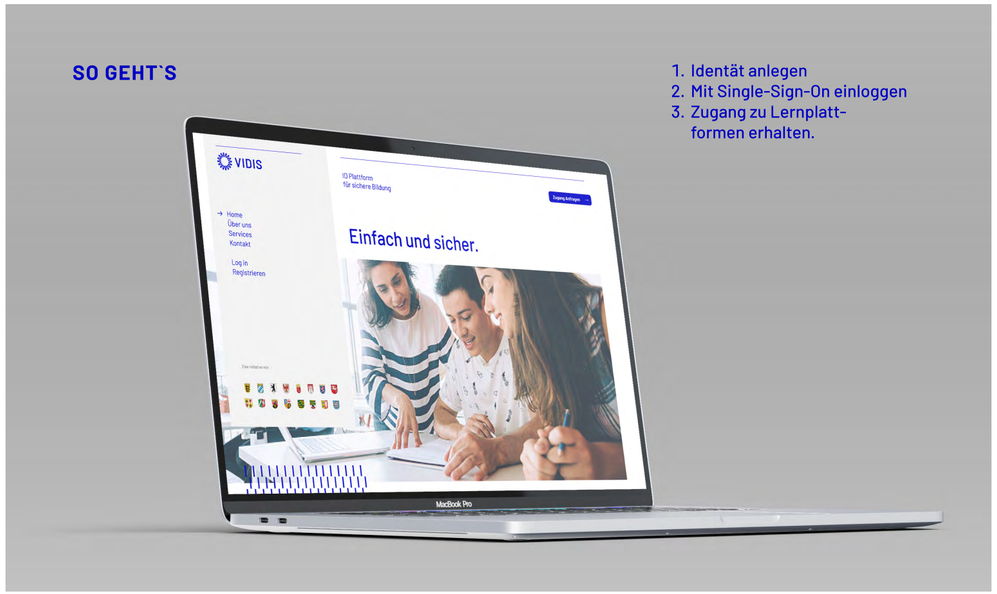
Dashboard


Dashboard
Dashboard
Customers
Schedules
Analytics
Help
Add New
Delete
Print
Export
Name
Email
Title
Date
Anzahl
Michael Scott marshall@yahoo.com Lehrer 07/04/1927 16
Dwight Schrute dwight@yahoo.com Lehrer 05/12/1983 15
Jim Halpert miles@mail.com Lehrer 08/08/1921 11
Pam Beesly barber@gmail.com Director 26/08/1949 11
Stanley Hudson gamble@outlook.com Assistenz 19/10/1992 16
Kevin Malone castaneda@mail.com Lehrer 01/02/1952 16
Angela Martin ryan@mail.com Schüler 05/12/1997 14
Phyllis Vance hendricks@yahoo.com Schüler 25/12/2012 16
Meredith Palmer kelly@mail.com Director 17/09/1971 13
Performance
heute
heute
Dwight +7%
Jim +1%
Stanley +2%
Phyllis -3%
Andy -9%

VIDIS

www.vidis.schule

VIDIS Login



ANLAGE 5:

Ansprechpartner

n.n. («Diensteanbieter»)

Kontaktperson technisch

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

Stellvertretung Kontaktperson technisch*

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

Kontaktperson Leitung

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

Stellvertretung Kontaktperson Leitung*

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

Kontaktperson Notfall*

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

*** Angabe fakultativ**

Änderungen der Kontaktangaben sind dem Identitätsvermittler umgehend nach Bekanntwerden anzuzeigen.

FWU Institut für Film und Bild in Wissenschaft und Unterricht gGmbH
vertreten durch die Geschäftsführer Michael Frost, Rüdiger Nill
HR: AG München B 2636
Bavariafilmplatz 3

82031 Grünwald

(«Identitätsvermittler»)

Kontaktperson technisch

Vorname	Markus
Name	Streicher
Adresse	Bavariafilmplatz 3 82031 Grünwald
E-Mail-Adresse	Markus.streicher@fwu.de
Telefonnummer	+49 (0)89 6497 258

Stellvertretung Kontaktperson technisch*

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

*** Angabe fakultativ**

Kontaktperson Leitung

Vorname	Michel
Name	Smidt
Adresse	Bavariafilmplatz 3 82031 Grünwald
E-Mail-Adresse	Michel.smidt@fwu.de
Telefonnummer	+49 (0)89 6497 352

Stellvertretung Kontaktperson Leitung*

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

Kontaktperson Notfall*

Vorname	
Name	
Adresse	
E-Mail-Adresse	
Telefonnummer	

ANLAGE 6: (LEER)

ANLAGE 7:

Technische Prüfung der Anbindung (Diensteanbieter)

Testen der Anbindung

Zum Testen Ihrer Anbindung rufen Sie Ihre "**BASE-URL**" auf. Das leitet Sie auf den VIDIS-Login.

Dort müssen Sie das **Test-Landesportal(IdP)** auswählen und sich mit unserem Test Account einloggen, danach sollten dann bei erfolgreichem Login in Ihrem System authentifiziert sein und Zugriff auf alle freigegebenen Inhalte haben.

Test Account Daten:
Username: den Usernamen erhalten Sie separat

Passwort: das Passwort erhalten Sie separat

Userinfo überprüfen

Über den endpoint https://aai.vidis.schule/auth/realms/vidis/.well-known/openid-configuration/userinfo können Sie sich die Übermittelten Userdaten unsererseits ansehen.

Das funktioniert wie folgt.

Schritt 1: Zuerst muss ein Token generiert werden.

Dieser Token (access_token) fungiert als "Bearer Token" der zum Abruf der User Info genutzt werden kann und zu Debugging zwecken, der Redirect Flow wird bei der finalen Integration verwendet.

```
curl --location --request POST 'https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'username=YYYYY' \
--data-urlencode 'password=XXXXX' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'client_id=account'
```

Schritt 2: Jetzt lassen sich die Userdaten mit dem Token abrufen

```
curl --location --request GET 'https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/userinfo' \
--header 'Authorization: Bearer <TOKEN>
```

oder alternative zu Schritt 2 wäre es den JWT Token zu dekodieren, um die Nutzerdaten auslesen zu können. Hierzu kann beispielsweise auch ein entsprechendes Online Tool verwendet werden (z. B. über https://devtoolzone.com/decoder/jwt, https://jwt.io/ etc.), sofern es sich nicht um reale Nutzerdaten handelt.

Per Code kann ein JWT Token beispielsweise wie folgt dekodiert werden:

```
import org.Apache.commons.codec.binary.Base64;
@Test
  public void testDecodeJWT(){
    String jwtToken
= "eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0ZXN0Iiwicm9sZXMiOiJST0xFX0FETUlOIiwiaXNzIjoibXlzZWxmIiwi
ZXhwIjoxNDcxMDg2MzgxfQ.1El2haSz9aMsHjFUXNVz2Z4mtC0nMdZo6bo3-x-aRpw";

    String base64EncodedHeader = split_string[0];
    String base64EncodedBody = split_string[1];
    String base64EncodedSignature = split_string[2];

    Base64 base64Url = new Base64(true);
    String header = new String(base64Url.decode(base64EncodedHeader));
    System.out.println("JWT Header : " + header);
    String body = new String(base64Url.decode(base64EncodedBody));
    System.out.println("JWT Body : "+body);
  }
```

Im Pilotbetrieb werden die Userdaten im ID token und per userinfo-endpoint übermittelt.

Das Ergebnis ist ein JSON mit den folgenden Userdaten.


```
{
 "exp": 1668155380,
 "iat": 1668155080,
```

```
 "auth_time": 0,
 "jti": "0a081ce3-5e15-4d85-9919-4ec95c2051ea",
 "iss": "https://aai-test.vidis.schule/auth/realms/vidis",
 "aud": "client-alias",
 "sub": "f3738cf7-a646-4bd7-af61-4a4c9e8151ef",
 "typ": "ID",
 "azp": "client-alias",
 "session_state": "b6b0b7f9-daf6-4377-a2e6-965f3356b3ba",
 "acr": "1",
 "sid": "b6b0b7f9-daf6-4377-a2e6-965f3356b3ba",
 "rolle": "LEHR",
 "schulkennung": "DE-LAND-12345",
 "bundesland": "DE-LAND",
 "heimatorganisation": "DE-LAND-Schulportal"
}
```


Integration VIDIS Login

Der VIDIS Button wird als Web Componente angeboten und ist über einen kleinen Codeschnipsel einzubinden. Die Scriptdatei liegt auf einem Server in einem unserer Rechenzentren. Sie können die JS-Datei entweder über unser CDN einbinden oder Runterladen und direkt in ihr Projekt integrieren.

JS-Link (CDN): **https://repo.vidis.schule/repository/vidis-cdn/latest/vidisLogin.umd.js**

Example - Einbindung des Buttons via Web Component

```
<!DOCTYPE html><meta charset="utf-8" /> <title>vidisLogin demo</title>
<script src="./vidisLogin.umd.js"></script>
<link rel="stylesheet" href="./vidisLogin.css" />
<vidis-login></vidis-login>
```

Gibt es weitere Technologien, in die sie den VIDIS Login einbinden möchten?

Dann lassen Sie uns das unbedingt wissen!

ANLAGE 8:

Dokumentation

Folgende Dokumente sind im Rahmen der Prüfung der Teilnahmevoraussetzungen bereitzustellen und laufend aktuell zu halten:

- Bereitstellung des geschlossenen Auftragsverarbeitungsvertrags zwischen Verantwortlichen und Diensteanbieter bzw. Bereitstellung des üblicherweise verwendeten Auftragsverarbeitungsvertrag (Muster).
  .
- Dokumentation der getroffenen technischen und organisatorischen Maßnahmen (TOM), Art. 32 DSGVO, § 64 BDSG.
- Zusammenfassung des IT-Sicherungskonzepts mit einer Übersicht der Rollen und des Rechtemanagements.
- Aufbewahrungs- und Löschkonzept.
- Diejenigen Vertragstexte mitsamt Anlagen, die zur Erbringung des digitalen Bildungsangebots mit den Käufern des digitalen Bildungsangebots üblicherweise abgeschlossen werden, ausgenommen Information, an denen ein berechtigtes Interesse an der Geheimhaltung besteht (bspw. Preiskalkulationen, Lizenzverträge, EVB-IT-Verträge). Allgemeine Geschäftsbedingungen oder Nutzungsbedingungen genügen. Distributoren von digitalen Bildungsangeboten erbringen die Vertragstexte mitsamt Anlagen im Verhältnis zu Ihren Diensteanbietern, ausgenommen Information, an denen ein berechtigtes Interesse an der Geheimhaltung besteht.
- Der Diensteanbieter übermittelt dem Identitätsvermittler zum Zwecke der Erbringung des Vermittlungsdienstes zu allen benötigten Daten die Zwecke und alle weiteren Angaben, die informationsrechtlich zu erbringen sind.
- Verfahren zum Umgang mit rechtswidrigen Nutzerinhalten.
- Verzeichnis der Datensicherheitsverstöße (Das Verzeichnis wird vertraulich behandelt).

WIR BEHALTEN UNS VOR DIESE DOKUMENTE NACH RÜCKSPRACHE MIT IHNEN WEITERZULEITEN.