EDK | CDIP | CDPE | CDEP |
Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de l'instruction publique
Conferenza delle direttrici e dei direttori cantonali della pubblica educazione
Conferenza da las directuras e dals directurs chantunals da l'educaziun publica

Beschluss Plenarversammlung | 22. Juni 2023

Datenföderation für die Berufsbildung; Abschluss der Konzeptionsphase und Verzicht auf die Realisation: Beschlussfassung

Das Generalsekretariat berichtet:

1 Die Plenarversammlung hat der Fachagentur Educa am 24. Juni 2021 den Auftrag erteilt, in Zusammenarbeit mit den Gremien und Fachorganisationen der Berufsbildung ein Konzept für eine schweizweite Datenföderation in der Berufsbildung auszuarbeiten. Diese soll den Datenaustauch in der Berufsbildung schweizweit vereinfachen und eine bessere Nutzung der Daten ermöglichen.

2 Zur Erarbeitung des Konzeptes für die Datenföderation genehmigte die Plenarversammlung insgesamt 375'000 CHF, das Staatssekretariat für Bildung, Forschung und Integration (SBFI) steuerte den gleichen Betrag bei.

3 Educa hat am 1. März 2023 die Konzeptionsphase abgeschlossen und dem SBFI und Generalsekretariat das dreiteilige Detailkonzept eingereicht. Das Konzept zum Aufbau der Datenföderation zeigt auf, wie Datenflüsse in Zukunft in der Berufsbildung organisiert werden können. Es präsentiert eine gesamtschweizerische Systemarchitektur und diskutiert die Auswirkungen von neuen datenschutzrechtlichen Prinzipien, wie sie beispielsweise im neuen Datenschutzgesetz des Bundes enthalten sind. Das Konzept unterstreicht insgesamt die Notwendigkeit der Klärung verschiedener zukunftsweisender Fragen, so zum Beispiel, wie die digitale Verifizierung von Ausbildungsnachweisen in der Berufsbildung geschehen kann.

4 Aufgrund der komplexen Ausgangslage, der grossen Tragweite des Vorhabens und anderweitigen Prioritäten in der Berufsbildung schlägt das Generalsekretariat in Absprache mit dem SBFI aber vor, von der Realisierung der Datenföderation abzusehen. Die Diskussion des Konzeptes für die Datenföderation in den Gremien der Berufsbildung hat gezeigt, dass es Educa nicht gelungen ist, die kantonalen Vertretungen der Berufsbildung vom Projekt zu überzeugen. Hingegen sollen laufende Projekte, welche das Datenmanagement in der Berufsbildung zum Thema haben, priorisiert werden.

5 Für die ursprünglich ab Oktober 2022 vorgesehenen Realisierungsphase der Datenföderation sind bereits Kantonsbeiträge von 83'333 CHF in Rechnung gestellt worden. Diese sollen für künftige Digitalisierungsprojekte zurückgestellt werden. Die im Budget 2023 eingestellten Mittel (500'000 CHF) werden den Kantonen nicht in Rechnung gestellt. Das Budget 2024 und der Finanzplan wird entsprechend angepasst.

6 Ab Juli 2023 soll zwischen der Fachagentur Educa und den Akteuren der Berufsbildung geklärt werden, ob einzelne Elemente des bisherigen Konzeptes als Teilprojekte («Inkremente») in Zukunft realisiert werden können. Diese werden SBFI und EDK gegebenenfalls zum Entscheid vorgelegt.

Die Plenarversammlung beschliesst:

1 Das Detailkonzept zum Abschluss der Konzeptionsphase des Projektes «Datenföderation für die Berufsbildung» wird zur Kenntnis genommen.

2 Die Realisierungsphase der Datenföderation in der Berufsbildung wird nicht eingeleitet. Die den Kantonen bereits in Rechnung gestellten 83'333 CHF werden für Digitalisierungsprojekte zurückgestellt.

Generalsekretariat | Secrétariat général
Haus der Kantone, Speichergasse 6, Postfach, CH-3001 Bern
+41 31 309 51 11, edk@edk.ch, edk.ch

Bern, 22. Juni 2023

Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren
Im Namen der Plenarversammlung:

sig.
Susanne Hardmeier | Generalsekretärin

Anhang:
- Konzept der Datenföderation für die Berufsbildung

Zustellung an:
- Konferenzmitglieder
- SBBK
- KOP
- Educa
- SBFI

Dieser Beschluss wird auf der Website der EDK publiziert.

232.32-14.3 bee

educa

Erlachstrasse 21
3012 Bern

+41 31 300 55 00
info@educa.ch

Konzept der Datenföderation für die Berufsbildung
Teil 1 – Ausgangslage und Architektur

15.11.2022

Digitaler Bildungsraum Schweiz
Espace numérique suisse de formation
Spazio formativo digitale svizzero
Spazi da furmazium digital svizzer
Swiss digital education space

educa

Inhalt

Management Summary

Seit Juni 2021 beschäftigt sich die Fachagentur Educa im Auftrag der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK) und des Staatsekretariats für Bildung, Forschung und Innovation (SBFI) mit der Konzeption einer Datenföderation für die Berufsbildung. Die Datenföderation soll den Zugang zu und den sicheren Austausch von Daten vereinfachen. Daten werden dabei als strategische Ressource für die Berufsbildung angesehen, in welchen grosses Innovationspotenzial steckt. Letztlich wird das Ziel verfolgt, die Daten schweizweit effizient auszutauschen sowie möglichst alle bestehenden Daten in einem Vertrauensraum zugänglich und für das gesamte System respektive für alle Verbundpartner nutzbar zu machen. Die Datenföderation ist als Gesamtarchitektur zu verstehen, die die Art und Weise, wie Daten in der beruflichen Grundbildung dereinst ausgetauscht werden, definieren wird. Sie dient damit auch für bestehende Dienste als Zielarchitektur.

Der Zugang zu Daten ist für alle Verbundpartner der beruflichen Grundbildung – für ihre Entscheid- Entwicklungs- und Innovationsmöglichkeiten – von eminenter Wichtigkeit. Datenzugang ist ein Innovationsmotor. Die aktuelle Geschwindigkeit, mit der Ereignisse wie Bildungsabschlüsse einzelner Lernender, Zuteilungsentscheide zu Berufsfachschulen, Kursdaten für Berufsbildner und Berufsbildnerinnen, finanzielle Verbindlichkeiten, Informationen zu neuen Ausbildungsinhalten etc. schweizweit zur Verfügung stehen, limitiert massgeblich das Innovationspotential der Arbeitswelt mit Bezug zur Berufsbildung.

Das Konzept der Datenföderation hebt die Möglichkeiten der Bereitstellung von Information zugunsten der beruflichen Grundbildung auf ein neues Niveau. Die Datenföderation stellt sich damit ganz in den Dienst der Innovationsfähigkeit des Schweizer Berufsbildungssystems, **indem sie zugunsten aller Verbundpartner Ereignisse direkt, autonom und ohne Umweg mit dem Nutzungskontext verbindet**. Im Fokus des Konzeptes stehen Lernende und Ausbildungsorte.

Die Projektziele gemäss Projektauftrag konnten in das Architekturkonzept übertragen werden. Geschärft wurde der Aspekt des künftigen Innovationspotentials für die berufliche Grundbildung. Zudem werden die Anforderungen von Lernenden und der Arbeitswelt in der Datenföderation stärker gewichtet. Und nicht zuletzt werden mit dem Architekturkonzept Notwendigkeiten mit Blick auf das kommende neue Datenschutzgesetz integriert.

Das vorliegende Dokument beinhaltet den ersten von drei Teilen der Konzeption einer Datenföderation für die Berufsbildung. Er zeigt die technische Architektur einer künftigen Datenföderation. In den beiden weiteren Teilen wir das Konzept des dazu nötigen Governance-Models und die für dessen Umsetzung gegebenenfalls nötigen gesetzlichen Grundlagen thematisiert. Zusammen mit einer Realisierungsplanung (insbesondere Zeitplan und Budgetierung) bilden die drei Konzeptteile zusammen das Entscheiddossier zuhanden SBFI und EDK.

1. Einführung

Der Bildungsraum Schweiz ist vielfältig und durchlässig. Individuen bewegen sich in analogen und digitalen Welten, haben zahlreiche Kontakte und produzieren an unterschiedlichsten Stellen Daten. Seit Juni 2021 beschäftigt sich die Fachagentur Educa im Auftrag der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK) und des Staatsekretariats für Bildung, Forschung und Innovation (SBFI) mit der Konzeption einer Datenföderation für die Berufsbildung. Daten werden dabei als strategische Ressource für die Berufsbildung angesehen, in welchen grosses Innovationspotenzial steckt. Letztlich wird das Ziel verfolgt, die Daten schweizweit effizient auszutauschen sowie möglichst alle bestehenden Daten in einem Vertrauensraum zugänglich und für das gesamte System nutzbar zu machen.

Durch einen dezentralen Aufbau bietet eine Datenföderation direktere Kommunikationswege für den Datenaustausch, erhöht dadurch die Widerstandsfähigkeit und verringert die Risiken des Berufsbildungssystems (bspw. den Ausfall eines zentralen Dienstes). Somit ist unter einer Datenföderation ein System von losen gekoppelten teilnehmenden Anwendungen und Datenbanken zu verstehen, welches durch eine dezentrale Infrastruktur unterstützt wird. Diese dezentrale Infrastruktur stellt die notwendigen Vertrauensdienste und Konsensfindungsmechanismen für die Funktionsfähigkeit der Datenföderation zur Verfügung.

1.1 Projektauftrag zur Konzeption einer Datenföderation in der Berufsbildung und der Vorbereitung der gesetzlichen Grundlagen

Als Fachagentur der EDK und des SBFI erhielt Educa im Juni 2021 durch die EDK-Plenarversammlung und die Direktion des SBFI den Projektauftrag[1] zur *Konzeption einer Datenföderation für die Berufsbildung* und *der Vorbereitung der entsprechenden gesetzlichen Grundlagen*. Gleichzeitig wurde dieses Projekt Teil des Aktionsplans zur Strategie Digitale Schweiz[2].

Folgende Projektziele formuliert der Projektauftrag für die Datenföderation:

1. Der Datenaustausch zwischen den Akteuren der Berufsbildung erfolgt hindernisfrei, ohne Verzögerung und in guter Qualität.
2. Datenbasierte Innovationspotentiale sind schweizweit für das Berufsbildungssystem zugänglich gemacht.
3. Daten werden als strategische Ressource für das Berufsbildungssystem schweizweit genutzt.
4. Das Vorhaben liefert einen Beitrag zur Innovationsfähigkeit des Berufsbildungssystems.

Das Projekt wird durch den Koordinationsausschuss Digitalisierung in der Bildung (KoA Digi) gesteuert. Die Projektleitung obliegt Educa. Das erarbeitete Konzept zur Datenföderation in der Berufsbildung soll wiederum durch die EDK-Plenarversammlung und die Direktion des SBFI diskutiert und gegebenenfalls beschlossen werden.

[1] https://edudoc.ch/record/220332/files/PB240621-foederation-d.pdf
[2] https://www.digitaldialog.swiss/de/datennutzungspolitik-fur-den-bildungsraum-schweiz

1.2 Einbezug der Verbundpartner

Für die Konzeption der Datenföderation in der beruflichen Grundbildung werden die Perspektiven aller Verbundpartner berücksichtigt. Der Bund ist für die strategische Steuerung und Entwicklung zuständig, die Kantone für die Umsetzung und Aufsicht. Die Organisationen der Arbeitswelt (OdA) sorgen für Bildungsinhalte und Ausbildungsplätze. Dass der Datenaustausch in der beruflichen Grundbildung erhebliches Verbesserungspotenzial aufweist, war und ist bei allen Verbundpartnern unbestritten. Educa hat sich im Laufe der Konzeptionsphase an folgenden Prämissen orientiert, die sich durch den Einbezug der Verbundpartner aufstellen liessen:

1. Die gegenwärtig laufenden Datenaustauschprojekte mit Bezug zu Datenaustauschprozessen (insb. HAKA, eCH-Datenstandard Berufsbildung, div. Register) sind wichtige Grundlagen.
2. Eine Reihe von zentral (kantonal, national) betriebenen Plattformen unterliegen einer «End-of-Life»-Thematik.
3. Es existiert kein schweizweiter Architekturansatz zur Verbindung existierender und künftiger digitaler Dienste.
4. Die Architektur der Datenföderation muss den föderalen Gegebenheiten der Schweiz und den jeweiligen Zuständigkeiten der Verbundpartner Rechnung tragen.
5. Mit Blick auf Datenzugang sind die Anforderungen der Kantone stark repräsentiert, die Anforderungen der Arbeitswelt und darin auch der Lernenden, sind hingegen bislang schwach gewichtet.

Damit diese Prämissen aufgestellt werden konnten, wurden die Anforderungen einer grossen Anzahl von Anspruchsgruppen aus den Reihen der Verbundpartner ermittelt. Ein erster Überblick dazu wurde bereits in der Initialisierungsphase Mitte 2020 bis Frühling 2021 geschaffen. Mit Beginn der Konzeptionsphase Mitte 2021 wurden die Austausche intensiver und systematischer.

Die Austausche mit den Verbundpartnern lassen sich wie folgt zusammenfassen:

1. Intensive Austausche mit den Mitgliedern der Schweizerischen Berufsbildungsämter-Konferenz (SBBK), insbesondere in zwei Austauschrunden Anfang März und Ende Mai 2021
2. Teilnahme an Gremiensitzungen der SBBK (Vorstand und Plenar) sowie der Kommission Organisation und Prozesse (KOP)
3. Bilaterale Gespräche mit allen Berufsbildungsämtern der Westschweiz und dem Tessin.
4. Gespräche mit kantonalen Berufsbildungsämtern der Deutschschweiz.
5. Kontinuierliche Austausche mit dem Schweizerischen Dienstleistungszentrum Berufsbildung (SDBB)
6. Kontinuierlicher Austausch mit einer Vielzahl von OdA, Dienstanbietern und Lehrbetrieben

7. Geringe Anzahl Gespräche mit Berufsfachschulen
8. Wiederkehrende Austausche mit dem Schweizerischen Arbeitgeberverband (SAV) und dem Schweizerischen Gewerbeverband (SGV) sowie dem Schweizerischer Gewerkschaftsbund (SGB) und Travail.Suisse.

Auf der strategischen Ebene hat Educa an zwei Sitzungen der Tripartite Berufsbildungskonferenz (TBBK) teilgenommen und hat Gespräche mit dem SBFI geführt. Zudem wurden systematisch Strategie-Dokumente auf Bundesebene (bspw. Aktionsplan Digitale Schweiz, div. Bundesratsberichte) und kantonale und interkantonale Grundlagendokumente (bspw. E-Government-Strategie Schweiz 2020–2023) ausgewertet und für die Konzeptionsarbeiten berücksichtigt.

1.3 Vorgehen

Die berufliche Grundbildung basiert auf einer Reihe von gesetzlichen Vorgaben, die auch mittels Datenaustauschprozessen umgesetzt werden. Verkürzt kann man sagen, dass diese Daten die berufliche Grundbildung widerspiegeln. Dieser Gedanke wird in den Mittelpunkt der Konzeption gestellt, er ist damit quasi die Architekturvision der Datenföderation. Für die Konzeption wendet Educa die TOGAF-Methode an (The Open Group Architecture Framework). Es handelt sich um ein etabliertes Vorgehensmodell zur Entwicklung von Unternehmensarchitekturen. Ziel der Architektur ist es, die Grundstrukturen der Datenföderation festzulegen und Regeln zu definieren, die das dynamische Zusammenspiel aller Komponenten koordinieren. Das Berufsbildungssystem soll dabei möglichst genau abgebildet werden. Durch die Diskussion über und das Formulieren von Architekturprinzipien wird das Fundament der neuen Strukturen geschaffen. Anschliessend können diverse Anwendungsfälle erstellt werden. Diese Zukunftsszenarien helfen, der Vielfalt des Berufsbildungssystems gerecht zu werden. Sie erlauben es auch den Datenaustausch nachvollziehen zu können und ihn sichtbar zu machen. Daraus lässt sich ableiten, welche technische Lösung und welche Governance für einen einfachen Zugang zu und einen verbesserten Austausch von Daten im Berufsbildungssystem geeignet sind.

Bei der Konzeption einer Datenföderation ist insbesondere der Einbezug aller Anspruchsgruppen wichtig (s. Kapitel 1.2.). Des Weiteren hat Educa intensiv die bestehenden Prozesse der Harmonisierung des Datenaustauschs zwischen den kantonalen Berufsbildungsämtern (HAKA) und in einer zweiten Runde die Entwürfe der HAKA-SOLL-Prozesse analysiert, die die SDBB erarbeitet hat (s. Kapitel 2.1.). Aufgrund der HAKA-Prozesse lässt sich die gesamte an den Datenaustauschprozessen beteiligte Stakeholder-Landschaft ableiten. Auch wurden bestehende technische Lösungen analysiert und mit den Anspruchsgruppen diskutiert. Ausserdem wurden rechtliche Grundlagen ausgewertet und analysiert (s. Kapitel 2.2.).

Um die Komplexität der Datenflüsse im Berufsbildungssystem zu vermindern, werden konkrete und zukunftsgerichtete Anwendungsfälle beschrieben. Der erste Anwendungsfall setzt einen Lernenden, Luca, ins Zentrum. In der Erläuterung des Anwendungsfalls werden vereinfachende Annahmen getroffen, so dass der Datenaustausch in einer künftigen Datenföderation analysiert werden kann, die technische Lösung bestimmt sowie Governance-Fragen sichtbar gemacht werden können.

Der vorliegende erste Konzeptteil fokussiert auf die technische Architektur einer künftigen Datenföderation. Diese technische Architektur wird zunächst anhand eines ersten Anwendungsfalls (s. Kapitel 3.1.) erzählt. Dann wird die Architektur technisch beschrieben (s. Kapitel 3.2.). Als drittes werden die Prinzipien der Architektur genannt (s. Kapitel 3.3.).

In den zwei geplanten weiteren Konzeptteilen (10. Januar 2023 und 1. März 2023) werden zunächst das Governance-Modell, also die Vorgaben und Mechanismen, die die Datenföderation dereinst steuern werden, vorgestellt. Auch werden weitere Anwendungsfälle erarbeitet. Darauf aufbauend wird aufgezeigt, welche gesetzlichen Grundlagen bereits existieren und welche gegebenenfalls zu schaffen wären, damit die Föderation in der beruflichen Grundbildung eingeführt werden kann. Auch wird im dritten Teil des Konzepts die Realisierungsplanung enthalten sein.

2. Ausgangslage

Das nächste Kapitel analysiert den bestehenden Datenaustausch in der beruflichen Grundbildung, zeigt die aktuellen rechtlichen Grundlagen und beleuchtet technologische sowie gesellschaftliche Entwicklungen.

2.1 Umfeldanalyse der beruflichen Grundbildung

Die Frage wie der Austausch von Daten in der beruflichen Bildung über Lernorte, Verantwortlichkeiten und Kantonsgrenzen hinweg vereinfacht und verbessert werden könnte, beschäftigt die Akteure der Berufsbildung bereits seit einiger Zeit. Anders als nationale Projekte und Programme konnten in den vergangenen Jahren viele Kantone partiell massgebliche Fortschritte im Datenaustausch in der beruflichen Bildung erzielen.

Die von einem Kanton verwendete Fachapplikation für die Datenverwaltung definiert und beschränkt gleichzeitig die Möglichkeiten des automatisierten Datenaustauschs. Um letzteren zu ermöglichen, haben sich einige Kantone dafür entschieden, dieselben Fachapplikationen zu verwenden, während andere Kantone stattdessen Schnittstellen eingerichtet haben. Dennoch gibt es zurzeit keinen automatisierten Datenaustausch zwischen sämtlichen Fachapplikationen und auch nicht zwingend innerhalb der gleichen Fachapplikation.

Abbildung 1 zeigt die in den kantonalen Berufsbildungsämtern eingesetzten Fachapplikationen und die daraus resultierenden Austauschgruppen. Die Deutschschweiz teilt sich in diejenigen Kantone, die ESCADA2 und diejenigen die KOMPASS 3 (im Verein «Interessengemeinschaft Informatik im Bildungswesen IGIB» organisiert) einsetzen. In der Westschweiz und im Kanton Tessin ist die Situation heterogener. Die Kantone Neuenburg und Jura nutzen dieselbe Lösung (CLOEE2), Freiburg und Tessin setzen IS-Academia ein, der Kanton Wallis ESCADA2 und die Kantone Genf und Waadt eigene Applikationen. Einige dieser Applikationen werden nur von Berufsbildungsämtern eingesetzt, andere auch für die Schulverwaltung (teilweise auch ausserhalb der beruflichen Grundbildung).

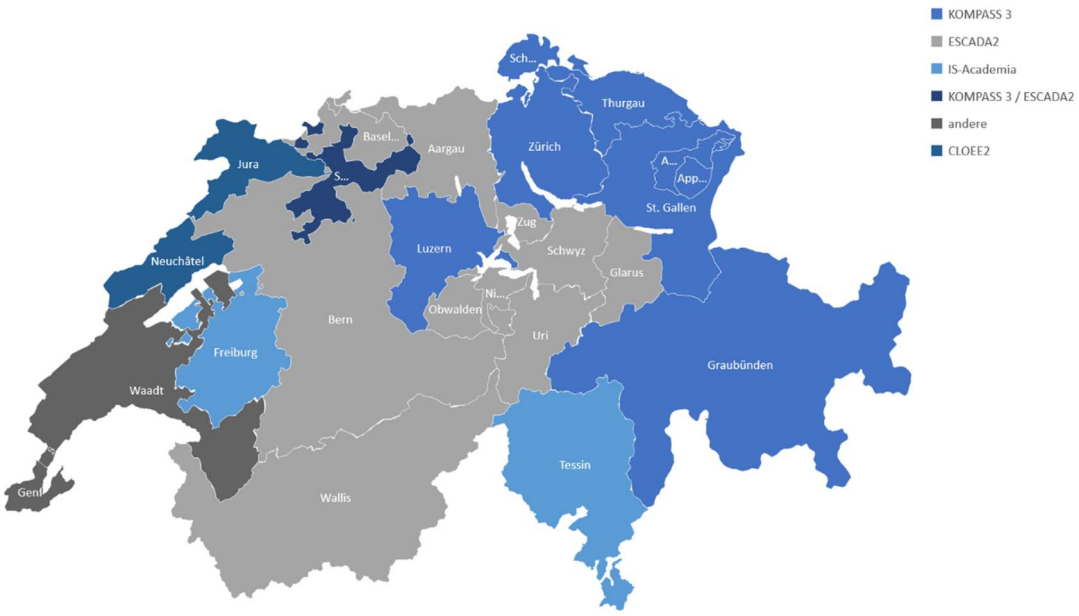

Abbildung 1: Genutzte Fachapplikationen in der Schweiz

Nachdem sich die Kantone in der SBBK Mitgliederversammlung vom 27. Mai 2020 für eine Anbindung der Berufsfachschulen an die kantonalen Systeme zum Datenaustausch ausgesprochen hatten, wurde von den Kantonen der IGIB ein Datenaustausch-Server, die sogenannte «Datendrehscheibe» entwickelt und im Herbst 2022 in Betrieb genommen. Diese ermöglicht erstmals den automatisierten Austausch von Daten zwischen den beiden Fachapplikationen ESCADA und KOMPASS.

Die kantonalen Berufsbildungsämter sind in der Regel der zentrale Drehpunkt des Datenaustauschs in der beruflichen Grundbildung. Bei ihnen liegt letztlich der Vollzug des Berufsbildungsgesetzes und über sie läuft ein Grossteil des Datenaustauschs, auch wenn sie nicht die primären Nutzniesser sind. Die Automatisierung des Datenaustausches ist bis anhin häufig nur in Teilen umgesetzt. Oft werden Daten zwischen kantonalen Berufsbildungsämtern und anderen Akteuren der beruflichen Grundbildung mittels Excel- oder PDF-Dateien ausgetauscht, die per E-Mail oder in Papierform verschickt werden. Dies ist mit einem erheblichen administrativen Aufwand sowie einer erhöhten Fehleranfälligkeit verbunden. Gründe hierfür liegen in der mangelnden Rechtssicherheit und Harmonisierung der Datenschutzrichtlinien, sowie der Heterogenität der eingesetzten Fachapplikationen. Zudem wird dieselbe Fachapplikation in verschiedenen Kantonen, und auch innerhalb eines Kantons, auf mehreren Ebenen der Berufsbildung teilweise unterschiedlich eingesetzt. Grund dafür sind individuelle Arbeitsweisen und Prozesse. Daten werden häufig mehrfach erfasst und in verschiedenen Systemen gespeichert, was in einer Minderung der Datenqualität resultiert. Diesen Zustand beschrieb die «Voranalyse optima», erstellt von der Haute école spécialisée de Suisse occidentale (HES-SO) im Jahr 2016. Umfragen der KOP bei den Berufsbildungsämtern im Oktober 2019 und März 2020 ergaben ein ähnliches Bild.

Es besteht ein breiter Konsens darüber, dass die derzeitige Situation nicht zufriedenstellend ist und dass die ergriffenen Massnahmen noch nicht ausreichen, um den schweizweiten Datenaustausch in der beruflichen Grundbildung effizient zu organisieren. Die SBBK hat aus diesem Grund das SDBB mit der Durchführung des Projekts «Harmonisierung interkantonaler Datenaustausch HAKA» beauftragt. Das SDBB erbringt bereits zentrale Leistungen im Zusammenhang mit dem Datenaustausch, hat Know-how zu den operativen Prozessen und ist bislang die einzige gemeinsame schweizweite operative Ressource für die kantonalen Berufsbildungsämter in diesem Kontext. Im Rahmen der Konzeptphase des Projekts HAKA wurde eine IST-Analyse der heutigen Geschäfts- und Datenaustauschprozesse der beruflichen Grundbildung in den Kantonen durchgeführt. Auf deren Grundlage wurden anschliessend harmonisierte SOLL-Datenaustauschprozesse erarbeitet, welche die Grundlage für künftige Umsetzungsprojekte bilden. Wie das SDBB jedoch bereits im Projektinitialisierungsauftrag selbst festgehalten hat, wird ein Nutzen von HAKA für die Berufsbildung erst dann in der Zukunft entstehen, «[…] wenn die in diesem Projekt erarbeiteten Ergebnisse auch tatsächlich eingesetzt und umgesetzt werden. Dies muss Teil von Nachfolgeprojekten [sein].»

Für die technische Übermittlung sowie die Sicherheit von Daten in der beruflichen Grundbildung gibt bis jetzt keine schweizweit verbindlichen Regelungen. Dagegen existieren mit den «Datenaustauschrichtlinien für die berufliche Grundbildung» seit Jahren nationale Richtlinien mit Anweisungen zu Inhalt und Form der in der beruflichen Grundbildung zu übermittelnden Daten. Diese Richtlinien, aktuell vorliegend in der Version 3.07a, basieren auf einem Konsens der Beteiligten und sind in allen Kantonen umgesetzt, wobei der Datenaustausch in wenigen Kantonen derzeit noch nach älteren Versionen erfolgt. Als Nachfolger der heutigen Datenaustauschrichtlinien wurde von der SDBB ein eCH-Standard für die Berufsbildung entworfen. Anfangs war dabei vorgesehen, die Datenaustauschrichtlinien weitgehend unverändert zu übernehmen und lediglich technisch als XML-eCH-Standard zu definieren. Da die heutigen Datenaustauschprozesse jedoch grosse Defizite aufweisen, wurde eine grundsätzliche Überarbeitung basierend auf den Ergebnissen vom Projekt HAKA notwendig. Zum Zeitpunkt der Redaktion des vorliegenden Berichts befindet sich der Standard eCH-0260 in der öffentlichen Konsultation und ein Kommittent der Amtsleitenden wird für die SBBK-Plenartagung im Februar 2023 angestrebt.

Die beschriebenen Projekte stellen zwar einen deutlichen Fortschritt im Vergleich zur im Projekt «optima» beschriebenen Situation aus dem Jahr 2016 dar. Gleichzeitig bleiben die bislang realisierten Lösungen fragmentarisch. In mehreren Austauschen mit Educa wurde durch alle involvierten Akteure das latente Bedürfnis nach einer Verbesserung und Automatisierung des schweizweiten Datenaustausches in der Berufsbildung geäussert. Dies betrifft den Austausch von Informationen zwischen kantonalen Verwaltungen, insbesondere mit der lateinischen Schweiz, aber auch schweizweit mit und zwischen Lehrbetrieben sowie OdA. Letztere haben in der Vergangenheit bereits wiederholt und an verschiedener Stelle die Notwendigkeit eines harmonisierten Datenaustausches über die drei Lernstandorte der beruflichen Grundbildung (Betriebe, Berufsfachschulen, überbetriebliche Kurse) angezeigt. Die anstehenden Reformen von KV und Detailhandel verstärken zusätzlich den Bedarf, valide Daten der Berufsfachschulen zu den Lernenden zu erhalten.

2.2 Die rechtliche Ausgangslage

Rechtsvorschriften wie beispielweise der bestehende rechtliche Rahmen für die berufliche Bildung (d. h. Bundesgesetz über die Berufsbildung, Verordnung über die Berufsbildung etc.) sowie der Datenschutz, vor allem auf kantonaler Ebene, sind für die Datenföderation von vorrangiger Bedeutung. In Bezug auf Blockchain-Technologien gibt es derzeit auf nationaler Ebene kaum konkrete Rechtsvorschriften. Verschiedene Gesetzesentwürfe sind jedoch in Arbeit (z. B. Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben, E-ID-Gesetz). Die datenschutzrechtlichen Konsequenzen eines solchen dezentralen Datenaustausches werden seit längerer Zeit intensiv diskutiert. So kommt beispielsweise das Europäische Parlament in einer Evaluation der Blockchain-Technologie zum Schluss, dass sie sich besser als zentralisierte Technologien zur Sicherung und Durchsetzung von Datenschutzstandards eignet. Neben der verteilten Speicherung personenbezogener Daten, wurden in der Evaluation weitere Vorteile der Technologie wie die Datenminimierung (z. B. durch sogenannte Zero-Knowledge-Proofs) und eine Automatisierung der Durchsetzung von Datenschutzgesetzen (z. B. mit Hilfe sogenannter intelligenter Verträge) aufgezeigt. Zusammen mit anderen Studien scheint sich ein Konsens darüber abzuzeichnen, wie solche Technologien rechtskonform eingesetzt werden können. Laufende Pilotprojekte bei den Kantonen befassen sich im Hinblick auf das revidierte Datenschutzgesetz ebenfalls mit der Frage, wie solche Vorteile im politischen und rechtlichen föderalen Kontext der Schweiz realisiert werden können.

In Anbetracht der immer deutlicher werdenden Hauptmerkmale der Architektur wird sich zeigen, wo Bedarf an gesetzlichen Grundlagen besteht. Darüber hinaus können die üblichen Instrumente des Bildungswesens zum Einsatz kommen (z. B. Organisationsreglement, Mitgliederverträge etc.). Zudem besteht basierend auf dem Artikel 48 BV die Möglichkeit interkantonale Verträge abzuschliessen. Auf diese Sachverhalte wird in späteren Konzeptteil eingegangen.

2.3 Technologische und gesellschaftliche Entwicklungen

Der effiziente Austausch und die darauf aufbauende vereinfachte Nutzung von bestehenden Datenbeständen ist ein zentrales Ziel der digitalen Transformation von Verwaltungen in Bund und Kantonen. Automatisierte Datenaustauschprozesse haben das Potential eine Entlastung von Datensubjekten zu ermöglichen und können die Qualität von Datenbeständen erhöhen. Dies erlaubt Behörden und öffentlichen Einrichtungen ihre Leistungen schneller, effizienter und kundenorientierter zu erbringen. Bislang wurden grosse Anstrengungen in die Skalierbarkeit solcher Systeme investiert, die sich in erster Linie auf die Bedürfnisse dieser Behörden konzentrierten.

Gleichzeitig wächst das Bewusstsein dafür, dass die soziale Akzeptanz und demokratische Legitimität von Systemen des automatisierten Datenaustausches auf lange Sicht nur gesichert werden können, wenn bei ihrer Konzeption und Umsetzung Fragen der Datensicherheit und der informationellen Selbstbestimmung stärker berücksichtigt werden. Sowohl in der Schweiz, wie auch im internationalen Kontext gewinnen daher Lösungsansätze an Bedeutung, die dem Einzelnen (dem Datensubjekt) mehr Kontrolle über ihre bzw. seine Daten geben. So kommt beispielsweise der Bundesrat auf Basis des Berichts zur öffentlichen

Konsultation zum «Zielbild E-ID» des Bundesamts für Justiz zum Schluss, dass die Prinzipien der «Datenhoheit beim Benutzer (Self Sovereign Identity)», der «Datensparsamkeit», des «Privacy by Design» (also der Implementierung des Datenschutzes durch die Datenarchitektur) und der dezentralen Datenspeicherung wesentliche Pfeiler einer künftigen E-ID-Lösung der Schweiz sein sollen. Das «Zielbild E-ID» löste mehrere Projekte in der Schweiz aus, die die Machbarkeit von digitalen Nachweisen prüfen (z. B. digitaler Führerschein, Bundespersonalausweis etc.). Auch im Bildungsbereich sind verschiedene Projekte im Gange, um das Potenzial der Blockchain-Technologien zu erforschen, z. B. bei der Überprüfung von Hochschulabschlüssen bei SWITCH.

International werden ähnliche Ansätze verfolgt, z. B. in der Europäischen Union mit dem «European Self Sovereign Identity Framework» als Teil der European Blockchain Services Infrastructure (EBSI). Dateninfrastrukturen, die auf dezentralen Prinzipien beruhen, eignen sich dabei nicht nur für die Verwaltung von Identitäten (Identity Management). In einem vor kurzem veröffentlichten White Paper schlägt beispielsweise die Wirtschaftskommission der Vereinten Nationen für Europa (United Nations Economic Commission for Europe, UNECE) die Verwendung einer solchen Architektur vor, um die Nachvollziehbarkeit und Transparenz im grenzüberschreitenden Warenverkehr zu verbessern. Eine Reihe von national und international tätigen Stiftungen und Konsortien, darunter das World Wide Web Consortium, digitalswitzerland, die Hyperledger Stiftung, IDunion oder die Stiftung Trust Over IP, haben zudem eine breite Palette an Normen und Anwendungsmöglichkeiten für Technologien identifiziert, die auf den Grundprinzipien von dezentralen Ansätzen beruhen. Mögliche Anwendungen wären der internationale Austausch von Gesundheitsdaten, die Verhinderung von Betrug bei der Auszahlung von Subventionen oder auch die Ausstellung überprüfbarer Hochschulzeugnisse. Gemeinsam ist allen Anwendungsmöglichkeiten, dass sie einen sicheren, transparenten, kontrollierbaren und nachvollziehbaren Austausch von Informationen ermöglichen, und damit Vertrauen im digitalen Raum generieren. Aufgrund dieser Eigenschaften sind Architekturen, die diese Prinzipien implementieren auch für den standardisierten Austausch von Daten attraktiv.

3. Die Architektur einer Datenföderation

Die Architektur einer Datenföderation beruht auf gemeinsamen Architekturprinzipien der Berufsbildung. Um die Datenflüsse analysieren zu können, wird ein konkreter Anwendungsfall konzipiert. Dieser wird anschliessend in der technischen Lösung abgebildet, damit die Zusammenhänge zwischen den Komponenten besser verstanden werden können. Während die technische Architektur regelt, welche Komponenten welche Vorgänge ausführen, müssen auch die Zuständigkeiten festgelegt und entsprechende Massnahmen verortet werden. Weitere Details zur Governance der Gesamtarchitektur werden im Teil II des Konzepts näher ausgeführt.

Ziel der Architektur ist es, die Grundstrukturen der Datenföderation festzulegen und Regeln zu definieren, die das dynamische Zusammenspiel aller Komponenten koordinieren. Das Berufsbildungssystem soll dabei möglichst genau abgebildet werden. Durch die Diskussion über und das Formulieren von Architekturprinzipien wird das Fundament der neuen Strukturen geschaffen.

Da es bei einer Datenföderation keine übergreifende Organisation oder Stelle gibt, die alle Aktivitäten steuert oder koordiniert, und eine Vielzahl von teilnehmenden Institutionen existieren, kann dieses Arrangement durchaus als Ökosystem bezeichnet werden. Die dezentralisierte Natur von Schlüsselkomponenten der Architektur gewährleistet zudem ein hohes Mass an Resilienz und Verfügbarkeit. Dies wird besonders für die Verankerung von Vertrauen in diesem digitalen Ökosystem gebraucht.

Die vorgeschlagene Architektur stellt die Lernenden in den Mittelpunkt aller Vertrauensbeziehungen und befähigt sie, ihre informationelle Selbstbestimmung zu verwirklichen. Dies ist ein bedeutender Beitrag zum Datenschutz, da es zu einem angemessenen Grad möglich ist, eine selektive Offenlegung zu realisieren. Es ist sogar möglich unter bestimmten Bedingungen Aussagen zu machen, ohne überhaupt Daten preiszugeben. Solche Details werden im nächsten Teil des Konzepts ausführlicher beschrieben.

3.1 Die Architektur als Anwendungsfälle: Digitale Nachweise in der beruflichen Grundbildung

Ein zentrales Konzept dieses architektonischen Ansatzes ist das des verifizierbaren, digitalen Nachweises. Dabei handelt es sich um eine oder mehrere von einer Organisation über eine Person gemachte Aussagen, welche in einer digitalen und verifizierbaren Form verpackt sind. Generell versteht man solche Nachweise als das digitale Gegenstück zu physischen Ausweisen und Diplomen. Datenübertragungen zwischen Parteien innerhalb der Datenföderation erfolgen meistens durch die Ausstellung von solchen digitalen Nachweisen an Inhaberinnen und Inhabern. Die Berechtigung als Ausgabestelle zu fungieren wird auf dem dezentralen Datenregister festgeschrieben. Die Inhaberin oder der Inhaber des digitalen Nachweises kann diesen wiederum an Dritte zur Verifizierung weiterleiten (ohne Einbezug der Ausgabestelle). Dies geschieht durch Einbezug des dezentralen Datenregisters. Damit kann überprüft werden, ob der digitale Nachweis von einer autorisierten Ausgabestelle stammt. Im Allgemeinen stellt die Ausgabestelle den Nachweis an jenes Subjekt aus, über welches die Aussage gemacht wurde, so dass Subjekt und Inhaber oder Inhaberin des digitalen Nachweises in der Regel dieselbe Person sind. Dies muss aber nicht immer der Fall sein, z. B. wenn eine Ausgabestelle einen digitalen Nachweis an die Erziehungsberechtigten eines Kindes ausstellt; in diesem Fall sind die Inhaber die Erziehungsberechtigten und das Subjekt ist das Kind.

Bevor ein solcher Datenaustausch stattfinden kann, muss ein Vertrauensverhältnis zwischen den kommunizierenden Parteien aufgebaut werden. Dies geschieht mit Hilfe eines dezentrales Datenregisters. Gestützt auf ein dezentrales Datenregister können Bildungseinrichtungen digitale Nachweise ausstellen und Lernende diese vorlegen. Dieses enthält die notwendigen öffentlichen Informationen, mit denen Dritte eine Überprüfung vornehmen können. Die Authentizität der digitalen Nachweise wird durch kryptographische Verschlüsselungsverfahren sichergestellt, was zusätzlich Vertrauen schafft. Für die Umsetzung eines solchen vertrauenswürdigen Datenregisters können verschiedene Technologien in Betracht gezogen werden. Im vorliegenden Beispiel ist eine öffentliche und eingeschränkte Blockchain, eine Art der dezentralen Datenspeicherung, vorgesehen. Ausgabestellen dürften auf diese Blockchain schreiben (daher eingeschränkt) und Überprüferinnen und Überprüfer könnten Daten auf

dieser Blockchain lesen, um Nachweise zu verifizieren (daher öffentlich). Der dezentrale Ansatz der Datenspeicherung – eines der Kernkonzepte einer Blockchain – wiederspiegelt den föderalen Charakter des Berufsbildungssystems somit auch in der Systemarchitektur.

Sämtliche durch Knoten durchgeführten Transaktionen entsprechen Ereignissen in der realen Welt (s. auch Kapitel 3.2.). Diese sind mit dezentralen Identifikatoren so abstrahiert, dass sie nur durch die Betroffenen nachgewiesen werden können. Aus diesem Grund liegt die Beweislast bei der bzw. dem Lernenden (also der Inhaberin oder dem Inhaber), wenn ein digitaler Nachweis vorgelegt wird. Die Prüfungsinstanz validiert nur den digitalen Nachweis sowie die damit verbundenen Transaktionen im dezentralen Datenregister. Bei der Überprüfung können mittels dezentralen Datenregisters keine Informationen über Lernende abgefragt werden (s. Abbildung 2).

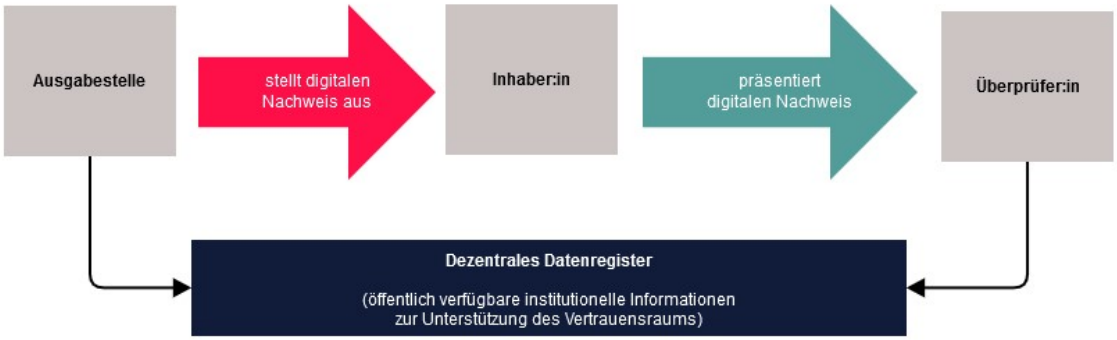

Abbildung 2: Digitale Nachweise

Lucas digitale Nachweise

Der folgende Anwendungsfall beginnt mit dem Lehrvertrag eines Lernenden. Nennen wir ihn Luca und nehmen an, dass er Schreiner mit Eidgenössischen Fähigkeitszeugnis werden möchte.

Luca erhält die Genehmigung des Lehrvertrags durch das Berufsbildungsamt auf herkömmliche Weise. Mit Genehmigung des Lehrvertrages beabsichtigt das Berufsbildungsamt ihm offiziell seinen Ausweis für Lernende auszustellen, diesmal in digitaler Form (s. Abbildung 3). Luca erhält, beispielsweise per Post oder E-Mail, einen für ihn generierten QR-Code, welchen er mit einer elektronischen Brieftasche scannt. Dabei handelt es sich um eine Software-Applikation für sein mobiles Endgerät. Damit der QR-Code nicht von einer beliebigen Person, die im Besitz des QR-Codes ist, gescannt werden kann, wird Luca durch das Berufsbildungsamt aufgefordert, seine Identität zu beweisen. Dies wäre z. B. möglich, in dem Luca ein bereits in seiner elektronischen Brieftasche vorhandener signierter Nachweis zeigt, der von einer vertrauenswürdigen Quelle ausgestellt wurde (z. B. eine E-ID). In dem der Lernende den QR-Code scannt und seine Identität mittels E-ID bestätigt, wird im Hintergrund ein kryptographisches Schlüsselpaar generiert. Dies bedeutet, dass für jede Partei ein privater und ein öffentlicher Schlüssel erstellt wird. Danach werden die öffentlichen Schlüssel ausgetauscht. Dadurch entsteht eine direkte und verschlüsselte Verbindung zwischen dem Berufsbildungsamt und Luca (sog. Peer-to-Peer-Vertrauensverhältnis). Damit entfällt die Notwendigkeit für Luca beim Berufsbildungsamt ein Konto anzulegen. Entsprechend entfallen auch die mit einem Konto verbundenen Identitätsmanagement-Risiken (z. B. Hackerangriff zum Diebstahl von Passwörtern). Ein solch dezentraler Ansatz zur Herstellung einer sicheren Verbindung zwischen zwei Parteien ist dadurch wesentlich sicherer als klassische Ansätze, die auf einer zentralen Autorität (z. B. einem Identitätsanbieter) basieren.

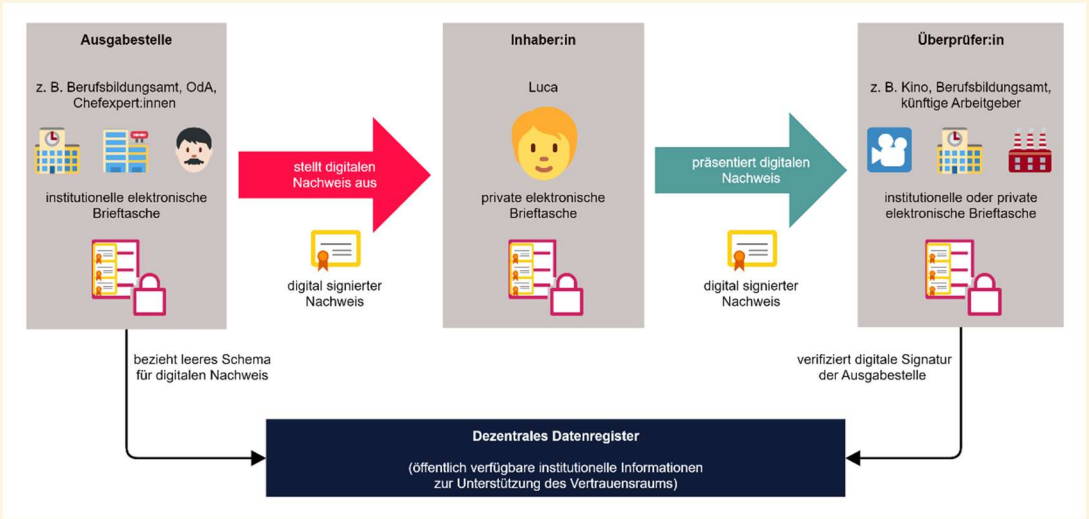

Abbildung 3: Anwendungsfälle von digitalen Nachweisen

Wurde, wie oben beschrieben, eine sichere Verbindung zwischen zwei Akteuren hergestellt, kann ein digitaler Nachweis übermittelt werden. In diesem Fall könnte also das Berufsbildungsamt (Ausgabestelle) Luca (Inhaber) den digitalen Ausweis für Lernende übertragen. Luca bewahrt diesen Ausweis in seiner elektronischen Brieftasche (neben weiteren digitalen Nachweisen) auf. Den Ausweis kann Luca beispielsweise bei einem Kinobesuch vorzeigen, um einen Rabatt zu erhalten. Dabei lässt Luca nur bestätigen, dass er in Ausbildung ist. Weitere Details, wie beispielsweise seinen ausgewählten Beruf oder sein Alter, liegen ausserhalb der Zweckbestimmung dieses Datenaustausches mit dem Kino und müssen deshalb nicht preisgegeben werden.

Die Gültigkeit von Lucas Ausweis ergibt sich aus folgenden Tatsachen:

- Sie wurde von einer vertrauenswürdigen, d. h. einer dazu berechtigten Stelle ausgestellt (z. B. Berufsbildungsamt),
- sie wurde in der Zwischenzeit nicht widerrufen (da keine Widerruf-Transaktion in einem für alle einsehbaren und dezentralen Datenregister zu finden ist) sowie
- aus weiteren relevanten Bedingungen (z. B. zeitliche Begrenzung des Nachweises).

Während seiner Ausbildung erhält Luca alle notwendigen Informationen, darunter auch Angaben zur Berufsfachschule, zu den überbetrieblichen Kursen und zum Lehrbetrieb, als digitaler Nachweis in seine elektronische Brieftasche. Muss Luca z. B. einen überbetrieblichen Kurs besuchen, dann erfolgt die Anmeldung bei der zuständigen OdA mit Hilfe der Angaben, welche er als digitale Nachweise bereits in seiner elektronischen Brieftasche hat (z. B. Ausweis für Lernende oder sonstige Kombinationen von digitalen Nachweisen, welche Luca zu einem Dossier zusammenstellen kann). Dabei muss kein Formular ausgefüllt werden. Stattdessen wird, wie oben beim Berufsbildungsamt, zuerst eine sichere Verbindung hergestellt, die die wahre Identität von Luca bestätigt.

Im Nachgang erhält Luca einen digitalen Nachweis, der seine Teilnahme am Kurs bestätigt. Diese Bestätigung wird sowohl in der institutionellen elektronischen Brieftasche der zuständigen Bildungseinrichtung als auch in Lucas persönlicher elektronischen Brieftasche aufbewahrt.

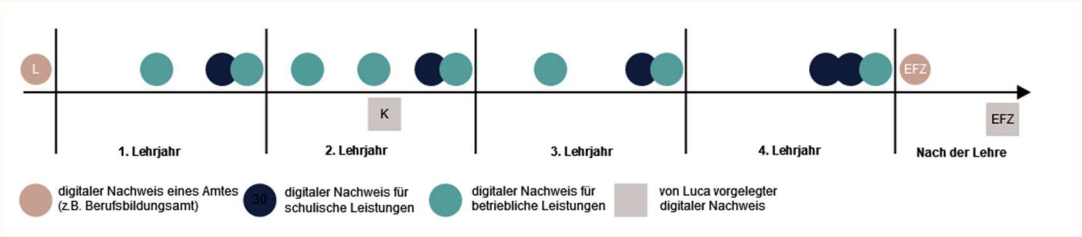

Abbildung 4: Digitale Nachweise im schulischen oder betrieblichen Kontext

Weitere Beispiele folgen demselben Muster: Es wird zuerst sichergestellt, dass eine direkte, sichere und verschlüsselte Vertrauensbeziehung besteht, und erst dann werden Aussagen über den schulischen (s. blaue Punkte in Abbildung 4) oder betrieblichen (s. grüne Punkte in der obigen Abbildung) Fortschritte von Luca in Form von digitalen Nachweisen gemacht. Dies gilt beispielsweise für die Herausgabe von Zeugnissen inkl. Prüfungsnoten oder Bestätigungen von individuellen praktischen Arbeiten bis hin zu gesamten Semesterzeugnissen oder Abschlüssen wie einem eidgenössischen Fähigkeitszeugnis -«Schreiner/in EFZ».

Das Vorhandensein jener Nachweise ermöglicht eine Entscheidungsfindung unter mehreren Parteien, ohne dass eine zentrale Behörde erforderlich ist. Dies wäre der Fall in der Berufsbildung, wo Bestätigungen seitens der Berufsfachschule, der OdA, des Lehrbetriebs und der Prüfungsexpertinnen oder Prüfungsexperten erforderlich sind, damit das EFZ für Luca ausgestellt werden kann. Zudem kann eine solche Entscheidungsfindung automatisiert werden (z. B. unter Berücksichtigung der Transaktionen im dezentralen Datenregister), womit administrative Fehler und Verzögerungen erheblich reduziert werden können.

Die Ausstellung eines EFZs kann wiederum weitere Transaktionsereignisse auslösen (z. B. kann ein ausgestellter Ausweis für Lernende als abgelaufen widerrufen werden). Ein einmal festgehaltener Sachverhalt kann zu jedem beliebigen Zeitpunkt in der Zukunft überprüft werden (z. B. wenn Luca nach seiner Ausbildung sich bei einem Arbeitgeber um eine Stelle bewirbt (s. «EFZ» Quadrat in der obigen Abbildung). Sollte sich hingegen herausstellen, dass der ausgestellte digitale Nachweis nicht korrekt war, kann dies durch den Widerruf dieses Nachweises berichtigt werden (d. h. Widerruf-Transaktion im dezentralen Datenregister).

Das Endergebnis ist, dass die Lernende bzw. der Lernende im Zentrum eines Geflechts von Vertrauensbeziehungen mit allen Lernorten und anderen Institutionen steht. Sie oder er erhält digitale Nachweise über wichtige Ereignisse des Qualifikationsverfahrens und kann gegebenenfalls solche Nachweise vorlegen, um diese zu belegen. Alle diese Daten sind in der persönlichen elektronischen Brieftasche sicher aufbewahrt. Wenn eine staatliche Aufgabe dies erfordert, können sie auch von den Behörden aufbewahrt werden. Da die Lernenden dadurch mehr Kontrolle über ihre Daten erhalten, ist es möglich, die Einhaltung des Datenschutzes besser zu gewährleisten.

3.2 Die technische Sicht auf die Architektur

Eine Architektur umfasst sämtliche Prozesse, Anwendungen, Datenbanken und deren Infrastrukturen, die zur Unterstützung eines bestimmten Betriebsmodells erforderlich sind. In diesem Kapitel werden die Kernelemente der Architektur einer Datenföderation beschrieben. Aus technischer Sicht ist eine Datenföderation ein Zusammenschluss unterschiedlicher Systeme, die dabei ihre Autonomie weitestgehend bewahren und in Abwesenheit einer zentralen koordinierenden Stelle ihre Aktivitäten organisieren können. Dies wird funktional so beschrieben, dass die oben erwähnten Anwendungsfälle und deren Umgang mit digitalen Nachweisen nachvollzogen werden können. Eine detailliertere Beschreibung der Prozesslandschaft und ihrer Abbildung auf Informationssysteme und Infrastrukturen erfolgt im Teil II der Konzeption einer Datenföderation für die Berufsbildung.

Folgendes Diagramm beschreibt eine vierschichtige Architektur zur Umsetzung der vorgeschlagenen Datenföderation:

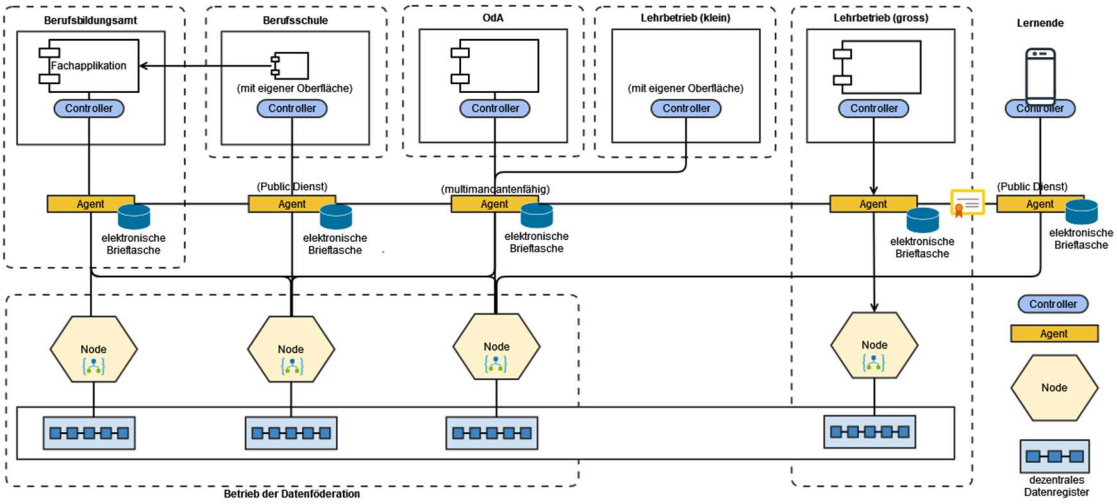

Abbildung 5: Vierschichte Architektur der Datenföderation

Dabei sind aus technischer Sicht insbesondere folgende Komponenten wichtig:

- Durch *Controller* wird es Personen und bestehenden Anwendungen ermöglicht, mit der Datenföderation zu interagieren. Dies umfasst die Validierung von Eingaben, die Koordinierung von Agenten und die Behandlung von Fehlern. Controller können eine Benutzeroberfläche anbieten (ähnlich wie Browser den Benutzerinnen und Benutzern die Interaktion mit dem Internet ermöglichen) oder in bestehende Fachanwendungen integriert werden.
- *Agenten* werden von Controller gesteuert und übersetzen die von ihnen erhaltenen Anweisungen in Transaktionen in der richtigen Reihenfolge für die Ausführung auf den Knoten. Agenten fungieren somit als Vermittler zwischen verschiedenen Programmen und kommen ohne direkte menschliche Interaktionen aus. Agenten nutzen eigene private Datenbanken (sog. elektronische Brieftaschen) zur Aufbewahrung von Personendaten inkl.

Nachweisen. Solche elektronischen Brieftaschen bestehen in unterschiedlichen Ausführungen sowohl für das massenhafte Ausstellen und Verwalten digitaler Nachweise (z. B. durch Institutionen) als auch für die Verwaltung individueller digitaler Nachweise (z. B. für Privatpersonen).

- Für die Ausführung von Transaktionen im dezentralen Datenregister sind *Knoten* zuständig. Jeder Knoten pflegt seine eigene Kopie des Datenregisters und aktualisiert diese auf Grundlage der Aktivitäten aller Knoten. Somit bilden Knoten ein Netzwerk zum Zweck der dezentralen Speicherung von transaktionalen Daten. Es ist auch möglich, dass die Knoten intelligente Verträge hosten, die als Reaktion auf bestimmte Transaktionen eine vordefinierte Logik ausführen. Ein solcher Code kann auch Benachrichtigungen an andere Parteien in Form von Ereignissen senden.
- Die Datenföderation nutzt ein *dezentrales Datenregister*. Dabei handelt es sich um ein öffentlich zugängliches und unveränderliches Register, das Aufzeichnungen wie auch die Erstellung und Überprüfung digitaler Nachweise unterstützt. Ein Datenregister verhält sich also wie ein Hauptbuch und ist nicht mit einer herkömmlichen Datenbank zu vergleichen. Sein einziger Zweck besteht darin, Transaktionen in der richtigen zeitlichen Abfolge aufzuzeichnen und diese Einträge vor nachträglichen Manipulationen zu schützen. Beispielsweise werden öffentliche Schlüssel von Ausgabestellen, Formatvorlagen für digitale Nachweise oder eine Liste mit widerrufenen digitalen Nachweisen allen zur Verfügung gestellt. Dabei geht es stets um Sachdaten – Personendaten werden nicht im dezentralen Datenregister gespeichert.

Es gibt viele mögliche Konfigurationen einer Datenföderation. Im obigen Diagramm werden entsprechend nur einige davon gezeigt. So ist es beispielsweise möglich, dass eine Bildungseinrichtung ihren eigenen Agenten betreibt oder dafür einen öffentlichen (mandantenfähigen) Agenten einsetzt. Darüber hinaus können die Knoten der Datenföderation von einem technischen Dienstleistungsanbieter betrieben werden. Möglich ist, dass auch grössere Organisationen ihre eigenen Knoten einbringen möchten und somit auch das dezentrale Datenregister bearbeiten würden.

Bestehende Systeme sollten nach Möglichkeit in die oben genannte Architektur (via Controller/Agenten) integriert werden. Dies ist insbesondere dann der Fall, wenn Anwendungen als massgebliche Quellen für kritische Daten dienen (z. B. DBLAP2). Die Datenübertragung muss jedoch nicht den üblichen, teilweise manuellen, Prozessen folgen. Möglich wäre, dass sie in Form von automatisierten Transaktionen erfolgen, die durch Ereignisse oder eine interne Anwendungslogik (z. B. intelligente Verträge) ausgelöst werden. Dadurch könnte beispielsweise ein digitaler Nachweis automatisch erstellt werden. Eine ereignisbasierte Architektur über direkte Verbindungswege scheint daher ein guter Ansatz zu sein.

3.3 Berücksichtigung der Architekturprinzipien

Die vorgeschlagene Architektur berücksichtigt mehrere Architekturprinzipien (AP), die die Datennutzung in der Berufsbildung steuern soll, und die bereits bildungspolitisch thematisiert wurden. Einer der wichtigsten Prinzipien ist die Förderung einer föderalistischen Datenhaltung (Architekturprinzip Governance AP.G.1), die die Daten als Vermögenswert für die Entscheidungsfindung versteht (AP.G.3). Dafür werden relevante Bildungsereignisse in Form

digitaler Nachweise den entsprechenden Parteien mittels eines dezentralen Datenregister zur Verfügung gestellt. Durch die verbesserte und zeitnahe Verfügbarkeit von Informationen (AP.G.2), die durch die Architektur ermöglicht wird, können Daten effizient ausgetauscht und genutzt werden. Die Verwendung von intelligenten Verträgen als Entscheidungsfindungsinstrumente verbessert zudem die Governance im Hinblick auf mehr Transparenz, Kohärenz und Verantwortung (AP.G.4). Dies ist insbesondere bei Transaktionen mit mehreren Parteien der Fall (z. B. wenn eine Berufsfachschule und ein Lehrbetrieb gemeinsam einen Entscheid treffen).

Das Vertrauen in die Berufsbildung entsteht aus allen legitimen Parteien (AP.G.5) und nicht nur durch die Bildungsbehörden. Dies wird durch die Identitätssicherung belegt (Architekturprinzip Sicherheit A.S.2, AP.S.3), was wiederum eine direkte Kommunikation zwischen den Parteien ermöglicht (Architekturprinzip Netzwerk AP.N.1), ohne dass die Daten vor der Verarbeitung zentralisiert werden müssen. Die vorgesehenen speziellen Sicherheitsmassnahmen ermöglichen somit, dass nur legitime Akteure an der Datenföderation beteiligt sind (AP.G.5, AP.S.1, AP.S.2 und AP.S.3). Diese tragen die volle Verantwortung für die in ihrem Namen durchgeführten Transaktionen (AP.G.4, Architekturprinzip Daten AP.D.1). Die technischen Massnahmen können durch weitere organisatorische Instrumente unterstützt werden (z. B. Organisationsreglement, Mitgliederverträge) und dienen auch zur Datenschutz-Rechtskonformität (AP.S.5). Beispielsweise fällt die Ausstellung von Zeugnissen in die Zuständigkeit der bestehenden Bildungsinstitutionen (z. B. Berufsbildungsamt, Berufsfachschule). Dagegen ist ihre Verifikation nicht nur eine Frage der Weiterleitung von digitalen Nachweisen, sondern setzt voraus, dass die betroffene Person ermächtigt wird, selbst zu entscheiden, welche Daten weiterzugeben sind. So gibt es in der Architektur Mechanismen, die eine selektive Offenlegung von Daten vorsehen. Weitere Mechanismen helfen zu prüfen, ob personenbezogene Daten in einer datenschutzkonformen Weise aufbewahrt werden.

2022 wurden folgende Prinzipien der Architektur entwickelt:

Referenz	Architekturprinzip (AP)
Governance im Sinne der Kontroll- und Steuerungsstrukturen: Dieses Prinzip sorgt dafür, dass sämtliche Datenbewegungen innerhalb der Gesamtarchitektur rechtens sind. Das Prinzip sieht Kontroll- und Steuerungsmechanismen vor, um die Rechtmässigkeit der Datenbewegungen sicherzustellen. Die Governance hat übergeordneten Charakter.	
AP.G.1	**Föderalistische Datenhaltung**: Die Datenföderation kommt ohne zentrale Datenspeicherung aus und ist föderalistisch organisiert. Dabei handelt es sich um einen Zusammenschluss von einzelnen Systemen ist, die ihre jeweilige Selbstständigkeit bewahren.
AP.G.2	**Konsensorientiertes Governance-Modell**: Dient der Akzeptanz und Legitimation der autonomen zugriffsberechtigten Entscheidungsträger. Das Prinzip muss die Agilität und das Funktionieren des Systems fördern, keinesfalls hemmen.
AP.G.3	**Verfügbarkeit von Daten bei Entscheidungsfindungen**: Das Prinzip geht davon aus, dass Entscheidungen erst richtig und rechtens getroffen werden können, wenn sämtliche relevanten Informationen verfügbar sind.

AP.G.4	**Transparenz, Integrität und Verantwortlichkeit über bildungsrelevante Ereignisse:** Mit diesem Prinzip wird die jederzeitige Revidierbarkeit der Daten gewährleistet. Die Revidierbarkeit der Daten entspringt einem legitimen potenziellen Bedürfnis der betroffenen Person, muss aber klaren Regeln gehorchen.
AP.G.5	**Legitimierter Zugang zur Datenföderation**: Nur wer ein legitimes Interesse an der Föderation hat, bekommt Zugang. Was ein legitimes Interesse ist, muss klar definiert werden. Die Rollen der verschiedenen Teilnehmenden müssen definiert, ihre Rechte im System müssen entsprechend festgehalten werden.

Sicherheit im Sinne des allgemeinen Zustandes, welcher als möglichst frei von (unvertretbaren) Risiken beurteilt wird. Die hier verfolgte Sicherheit ist die objektive Sicherheit (in Abgrenzung zur subjektiven Sicherheit), welche Risiken erkennt, deren Gefährdungspotenzial richtig einschätzt und effektiv entgegenwirkt.

AP.S.1	**Rollenbasierte Zugangskontrolle (RBAC)**: Damit soll sichergestellt werden, dass nur berechtigte (legitimierte s. AP.G.5) Personen, im Rahmen der ihnen zugeteilten Rollen Zugriff haben bzw. Änderungen vornehmen können.
AP.S.2	**Identitätssicherung der Komponenten**: Der Zugang zur Datenföderation muss auf vertrauenswürdige Teilnehmende beschränkt werden, die in der Lage sein müssen, ihre Identität nachzuweisen. Nur so können die erforderlichen datenschutzrechtlichen Prinzipien eingehalten werden. Bei diesem Architekturprinzip handelt es sich um den allgemeinen Zugang zur Föderation.
AP.S.3	**Identitätssicherung der betroffenen Parteien**: Über die allgemeine Identitätssicherheit des AP.S.2 hinaus, sorgt dieses Architekturprinzip für die bestätigte Legitimation der betroffenen Partei. Diese Zusatzhürde ist wichtig, weil die betroffene Partei gleichsam Eigentümer:in der bearbeiteten Daten ist. Nur sie soll Änderungen (Bearbeitungen) veranlassen dürfen.
AP.S.4	**Kontinuierliches Monitoring der Datenaustausche**: Es werden Instrumente/Mechanismen im System institutionalisiert, welche die Umsetzung der AP.S.1–3 kontinuierlich kontrollieren und sicherstellen. Dieses Architekturprinzip versucht Missbräuche schon im Vorfeld zu erkennen und zu verhindern.
AP.S.5	**Sicherer und rechtskonformer Datenaustausch**: Gemäss diesem Architekturprinzip wird ein technologischer «State of the Art» als Messlatte festgelegt. Damit werden hohe Standards sichergestellt.

Daten im Sinne von Zeichen, die eine Information enthalten. Wichtig in diesem Zusammenhang sind die Informationen, welche Personen im Bildungsbereich betreffen.

AP.D.1	**Daten sind ein gemeinsames Gut im Dienst der Berufsbildung**: Alleinige Eigentümer von Daten in der Bildung sind Lernende. Dieses Prinzip bringt die Notwendigkeit zum Ausdruck, dass Daten in der Bildung nicht von einzelnen Verwaltungsstellen gehortet werden. Sämtliche Bildungsinstitutionen (Lehrbetriebe, Berufsbildungsschulen usw.) stehen im Dienst einer effizienten und zielführenden Datenbearbeitung. Als Ausgabestellen dürfen diese Komponenten dem System keine Hindernisse in den Weg stellen.
AP.D.2	**Datenqualität ist Aufgabe der Komponente**: Eigenverantwortung und datenschutzrechtliche Verantwortlichkeit stehen sich gegenüber. Indem die Komponenten sicher identifiziert werden (AP.S.2–3) und ihnen eine klare Rolle zugeteilt wird (AP.S.1), kann bei Fehlern rasch die Verantwortlichkeit zurückverfolgt werden. Somit muss jede Komponente eigenverantwortlich innerhalb der Föderation handeln.

AP.D.3	**Semantische Interpretierbarkeit der Daten**: Dieses Prinzip sichert die korrekte Interpretation der Informationen (Daten); das Prinzip setzt eine gemeinsame Sprache sowie die jederzeitige Übersetzbarkeit anderslautende Begriffe in die gemeinsame Sprache voraus. Die semantische Interpretierbarkeit der Daten sorgt für Kontinuität, d. h. immer gleiche Bedeutungen der gleichlautenden eingegebenen Daten.
Netzwerk im Sinne. eines Systems mit einer zugrundeliegenden Struktur, welche sich modellieren lässt und die Mechanismen zur Selbstorganisation enthält.	
AP.N.1	**Direkter Datenaustausch**: Es ist wichtig, dass die einzelnen Komponenten des Netzwerkes unmittelbar (ohne Mittler) miteinander kommunizieren können. Nur so können sie zeitnah und effizient reagieren. Der direkte Datenaustausch unterstützt auch die Datenintegrität, indem die Datenbearbeitung direkt auf Veranlassung hin erfolgt (ohne Zwischenstufen). Dieses Prinzip setzt voraus, dass die AP.S.1–5 jederzeit eingehalten werden.
AP.N.2	**Atomarität von Bildungsereignissen**: Es ist wichtig Regeln auszudenken und zu implementieren, welche definieren, wann, inwiefern und zu welchem bindenden Zweck Bildungsereignisse offen verkündet werden dürfen. So wird die jederzeitige Aktualität der Daten sichergestellt
AP.N.3	**Asynchronität der Kommunikation**: Wann Daten übermittelt werden, spielt für das Netzwerk keine Rolle; Daten müssen jederzeit für jedermann einsehbar sein. Sobald Daten übergegeben werden, gelten sie.

4. Zwischenfazit

Der vorliegende erste Teil erläutert die Bedeutung des Einbezugs der Verbundpartner, die Vorgehensweise sowie die Ausgangslage für die Konzeption einer Datenföderation für die Berufsbildung. Des Weiteren wurde die konzipierte Architektur in unterschiedlicher Weise präsentiert. Einerseits helfen die Anwendungsfälle das Verständnis zur Thematik aufzubauen, andererseits wurden weitergehende technische Informationen gegeben. Die Konzeption stützt sich auf Architekturprinzipien, die mit den Verbundpartnern diskutiert wurden. Es soll der Zugang zu und den sicheren Austausch von Daten vereinfacht werden. Daten werden dabei als strategische Ressource für die Berufsbildung angesehen, in welchen grosses Innovationspotenzial steckt. Letztlich wird das Ziel verfolgt, die Daten schweizweit effizient auszutauschen sowie möglichst alle bestehenden Daten in einem Vertrauensraum zugänglich und für das gesamte System respektive für alle Verbundpartner nutzbar zu machen.

Die Projektziele gemäss Projektauftrag konnten in das Architekturkonzept übertragen werden. Geschärft wurde der Aspekt des künftigen Innovationspotentials für die berufliche Grundbildung. Zudem werden die Anforderungen von Lernenden und der Arbeitswelt in der Datenföderation stärker gewichtet. Und nicht zuletzt werden mit dem Architekturkonzept Notwendigkeiten mit Blick auf das kommende neue Datenschutzgesetz integriert.

Das vorliegende Dokument beinhaltet den ersten von drei Teilen der Konzeption einer Datenföderation für die Berufsbildung. Er zeigt die technische Architektur einer künftigen Datenföderation. In den beiden weiteren Teilen wir das Konzept des dazu nötigen Governance-Models und die für dessen Umsetzung gegebenenfalls nötigen gesetzlichen Grundlagen thematisiert. Zusammen mit einer Realisierungsplanung (insbesondere Zeitplan und Budgetierung) bilden die drei Konzeptteile zusammen das Entscheiddossier zuhanden SBFI und EDK.

Anhang

Begrifflichkeiten

Begriff	Definition
Agent	Ein Agent ist eine Softwarekomponente, die die Anweisungen eines oder mehrerer Controller verarbeitet, entsprechend in der Datenföderation weiterverbreitet, mit den Knoten kommuniziert oder digitale Nachweise (und damit personenbezogene Daten) speichert.
Ausgabestelle	Unter einer Ausgabestelle («Issuer») versteht man eine Stelle, die z. B. durch eine staatliche Institution autorisiert ist, digitale Nachweise auszustellen.
Betreiber:in	Dies können Institutionen, private oder juristische Personen sein, die Knoten betreiben.
Blockchain	Ein Ledger-Speichersystem, bei dem Transaktionsdaten angehängt werden und nicht nachträglich geändert werden dürfen. Blockchains werden durch ein Netzwerk von Knoten realisiert und sind daher in der Regel dezentralisiert.
Controller	Unter Controller versteht man eine Software-Komponente, die es Personen und Institutionen ermöglicht, über eine Benutzeroberfläche auf den Agenten zuzugreifen und so Zugang zu digitalen Nachweisen zu erhalten, das dezentrale Datenregister zu nutzen oder mit anderen Mitgliedern oder Teilnehmenden der Datenföderation zu kommunizieren.
Dezentrales Datenregister	Ein dezentrales Datenregister ist ein öffentlich zugänglicher und von allen lesbarer dezentraler Speicher, der alle notwendigen Informationen enthält, um eine Datenföderation im Allgemeinen und ein Ökosystem für digitale Nachweise im Speziellen betreiben zu können.
Dezentrale Identifikatoren	Eine Form der Identifikation, die in dezentralen Systemen verwendet wird und die Verknüpfung von Ereignissen mit Daten in einer Weise ermöglicht, dass nur die betroffenen Parteien jene Verknüpfungen herstellen können.
Elektronische Brieftasche	Bei einer elektronischen Brieftasche handelt es sich um eine Software-Applikation für die sichere Aufbewahrung digitaler Nachweise.
Inhaber:in	Unter Inhaberin oder Inhaber versteht man die Person oder Institution, die einen digitalen Nachweis elektronisch besitzt.
Intelligente Verträge	Intelligente Verträge sind Computerprogramme, die die automatisierte Bearbeitung von Daten und darauf basierend eine automatisierte Entscheidungsfindung entlang von vordefinierten Kriterien bewirken.
Knoten	Ein Knoten ist eine Verarbeitungsinstanz des dezentralen Datenregisters. Knoten tätigen, überprüfen und speichern Transaktionen auf dem dezentralen Datenregister und können zudem auch intelligente Verträge hosten.
Mitglied	Eine institutionelle Partei der Datenföderation, die aktiv mitwirken darf (z. B. Erstellen von Transaktionen). Solche Parteien müssen mit dem Betreiber der Datenföderation einen Vertrag unterzeichnen.

Teilnehmende	Eine Partei der Datenföderation, die passiv mitwirken darf (z. B. Einsicht von öffentlichen Informationen im dezentralen Datenregister oder die Verifikation von Nachweisen). Solche Parteien müssen mit dem Betreiber oder mit der Betreiberin der Datenföderation in der Regel keinen Vertrag unterzeichnet haben.
Transaktion	Eine Transaktion ist eine Operation, mit der Daten in das dezentrale Datenregister übernommen werden können. Transaktionen beinhalten keine personenbezogenen Daten.
Überprüfer:in	Unter einer Überprüferin oder einem Überprüfer versteht man Personen oder Institutionen, welche die Validität von ihnen vorgelegten digitalen Nachweisen mithilfe der Informationen auf dem dezentralen Datenregister überprüfen.
(verifizierbarer) digitaler Nachweis	Im vorliegenden Kontext beinhaltet ein digitaler Nachweis eine oder mehrere Aussagen einer Institution oder Behörde (z. B. einer Schule oder eines Amtes) zu einem Subjekt (z. B. einer Lernenden). Ob diese Aussagen aus vertrauenswürdiger Quelle stammen, kann mithilfe der Daten auf dem dezentralen Datenregister überprüft werden – daher verifizierbarer digitaler Nachweis.

educa

Erlachstrasse 21
3012 Bern

+41 31 300 55 00
info@educa.ch

Konzept der Datenföderation für die Berufsbildung
Teil 2 – Neue Datenparadigmen und Governance-Modell

10.1.2023

Digitaler Bildungsraum Schweiz
Espace numérique suisse de formation
Spazio formativo digitale svizzero
Spazi da furmazium digital svizzer
Swiss digital education space

educa

Inhalt

educa

Management Summary

Im ersten Teil des Konzepts der Datenföderation für die Berufsbildung wurde der Fokus auf die künftige technische Infrastruktur gelegt. Damit wurden die Aspekte der Effizienzsteigerung, der Datenverfügbarkeit und der Anschlussfähigkeit betont. Der zweite Teil des Konzepts nimmt einen anderen Blickwinkel ein. Neben dem Gebot der Effizienzsteigerung existiert durch den Paradigmenwechsel im Umgang mit personenbezogenen Daten ein weiterer wesentlicher Treiber, warum der Datenaustausch in der beruflichen Grundbildung neu gedacht werden sollte.

Das Thema «Daten» hat sich im Zuge der fortschreitenden digitalen Transformation gesellschaftspolitisch gewandelt, insbesondere wenn es sich um personenbezogene Daten handelt. Das neue Datenschutzgesetz auf Bundesebene läutet diesbezüglich in der Schweiz verschärfte Verpflichtungen gegenüber Datenverwaltenden ein. Sie werden dazu verpflichtet, betroffene Personen angemessen über die Beschaffung und Bearbeitung von Personendaten zu informieren. Dem Individuum werden künftig wesentlich weitreichendere Verfügungsrechte zugestanden, als dies bis anhin der Fall war. Gleichzeitig ist der Umgang mit personenbezogenen Daten noch stärker aus einer Individualperspektive zu beurteilen. Eine künftige, voraussichtlich öffentlich-rechtlich organisierte Datenföderation hat mit Blick auf ihr Innovationspotential diese Änderungen zu berücksichtigen. Wie dies in der Datenföderation ermöglicht wird, zeigt der Anwendungsfall «Ämter und Lernorte im Umgang mit Daten». Hier werden insbesondere «Toxische Daten» betrachtet. Als toxische Daten werden personenbezogene Daten verstanden, die im weitesten Sinne des Wortes – willentlich oder unwillentlich – unrechtmässig bearbeitet werden. Zahlreiche datenbearbeitende Akteure in der beruflichen Grundbildung machen diesen Aspekt besonders relevant. Die vorgeschlagene technische Architektur ermöglicht Strategien, um die durch die kommende Datenschutzregulierung geforderten Aspekte im Umgang mit Daten bewältigen zu können.

Dementsprechend benötigt die technische Infrastruktur einer Datenföderation für die Berufsbildung eine adäquate Governance. Dazu ist ein Data-Governance-Modell umzusetzen. Das Modell ist ein Rahmenwerk, das beschreibt, wie Mitgliederorganisationen ihre Daten verwalten, austauschen und nutzen. Es umfasst Regeln, Richtlinien, Prozesse und Systeme für die Erfassung, Speicherung, Auswertung, Archivierung, Weitergabe und Löschung von Daten sowie Richtlinien zur Gewährleistung der Qualität dieser Daten. Das Ziel des Data-Governance-Modells ist es somit, allen beteiligten Akteuren der Datenföderation eine kohärente, effektive Nutzung und einen sicheren Austausch von Daten zu ermöglichen.

Das Konzept der Datenföderation für die Berufsbildung fügt sich in eine im Aufbau befindende Landschaft vertrauenswürdiger, föderal organisierter Datenräume ein. Diese Datenräume sind national wie auch zunehmend international interoperabel ausgestaltet.

Das vorliegende Dokument beinhaltet den zweiten von drei Teilen der Konzeption einer Datenföderation für die Berufsbildung. Zusammen mit einer Realisierungsplanung (insbesondere Zeitplan und Budgetierung) bilden die drei Konzeptteile zusammen das Entscheiddossier zuhanden des Staatssekretariats für Bildung, Forschung und Innovation (SBFI) und der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK).

1. Einführung

Der erste Teil des Konzepts erläuterte die Bedeutung des Einbezugs der Verbundpartner, die Vorgehensweise sowie die Ausgangslage für die Konzeption einer Datenföderation für die Berufsbildung. Des Weiteren wurde die konzipierte Architektur in unterschiedlicher Weise präsentiert. Der vorliegende zweite Teil des Konzepts schlägt ein Governance-Modell für die Datenföderation vor, dass in Einklang mit den Forderungen der kommenden Datenschutzgesetzgebung ist. Anhand eines Anwendungsfalls im Zusammenhang mit toxischen Daten wird das Potenzial der vorgeschlagenen technischen Architektur beleuchtet, indem entsprechende Bewältigungsstrategien aufgezeigt werden.

1.1 Rekapitulation der technischen Architektur

Ziel der Architektur ist es, die Grundstrukturen der Datenföderation festzulegen und Regeln zu definieren, die das dynamische Zusammenspiel aller Komponenten koordinieren. Das Berufsbildungssystem soll dabei möglichst genau abgebildet werden. Eine Architektur umfasst sämtliche Prozesse, Anwendungen, Datenbanken und deren Infrastrukturen, die zur Unterstützung eines bestimmten Betriebsmodells erforderlich sind. Die technische Architektur der Datenföderation, welche in Teil I skizziert wurde, ist dezentral organisiert (s. Kapitel 3 in Teil 1).

Ein wesentlicher Aspekt des architektonischen Ansatzes des Konzepts ist der verifizierbare, digitale Nachweis. Dabei handelt es sich um eine oder mehrere von einer Organisation über eine Person gemachte Aussagen, welche in einer digitalen und verifizierbaren Form verpackt sind. Zudem basieren die Nachweise auf einem Vertrauensverhältnis, welches zwischen den kommunizierenden Parteien aufgebaut wird. Die Teilnehmenden der Datenföderation erhalten die digitalen Nachweise und können sie weitergeben.

Aus technischer Sicht ist eine Datenföderation ein Zusammenschluss unterschiedlicher Systeme, die dabei ihre Autonomie weitestgehend bewahren und in Abwesenheit einer zentralen koordinierenden Stelle ihre Aktivitäten organisieren können. Insbesondere die Komponenten Controller, Agent, Knoten und dezentrales Datenregister sind entscheidend.

Durch die Diskussion über und das Formulieren von Architekturprinzipien wird das Fundament der neuen Strukturen geschaffen. Die vorgeschlagene Architektur berücksichtigt mehrere Architekturprinzipien, die die Datennutzung in der Berufsbildung steuern sollen. Einer der wichtigsten Prinzipien ist die Förderung einer föderalistischen Datenhaltung (Architekturprinzip Governance), die die Daten als Vermögenswert für die Entscheidungsfindung versteht. Des Weiteren sind Architekturprinzipien mit Fokus auf Sicherheit, die Art und Qualität der Daten sowie als Netzwerk-System erarbeitet worden.

1.2 Zusammenarbeit mit den Anspruchsgruppen

Während für den Teil I des Konzepts das Wissen der Verbundpartner der Berufsbildung in hohem Masse integriert wurde, ist die Thematik des Teil II nur zum Teil spezifisch für die berufliche Grundbildung. Dank der Zusammenarbeit mit dem Schweizerischen Dienstleistungszentrum Berufsbildung (SDBB) konnte insbesondere der hier präsentierte Anwendungsfall

«Ämter und Lernorte im Umgang mit Daten nach einem Lehrabbruch» (s. Kapitel 4) detailliert realisiert werden. Das zentrale Thema - Datenschutz sowie dessen Implementierung in Architekturen wie der Datenföderation - ist hingegen ein Schwerpunktthema der Fachagentur. Educa besitzt hierzu wesentliches Fachwissen wie auch zur Frage, wie ein Data-Governance-Modell einer dezentralen Dateninfrastruktur im föderalen Bildungskontext idealerweise auszusehen hat. In enger Zusammenarbeit mit der Datenschutzbeauftragten des Kantons Zürich konnte zudem untersucht werden, wie die Datenföderation den Schutz von Personendaten in der Berufsbildung verbessern kann. Insbesondere wurde der Ansatz verfolgt, dass Daten eine Haftung für ihre Aufbewahrer nach sich ziehen könnten. Dafür müssen spezifische Bewältigungsstrategien entwickelt werden, die mittels der Datenföderation realisiert werden können. (s. Kapitel 2.3).

Die Architektur der Datenföderation steht im Einklang mit internationalen Normen, die den Ansatz für digitale Nachweise und die dazugehörigen dezentralen Identifikatoren standardisiert haben. Die Einhaltung solcher Normen gewährleistet ein hohes Mass an technischer Kohärenz und Interoperabilität mit anderen in der Schweiz entstehenden Ökosystemen (s. Kapitel 3.6).

Mit Blick auf die Entwicklung vertrauenswürdiger Datenräume und die Sicherstellung der Anschlussfähigkeit einer künftigen Datenföderation für die Berufsbildung wurde eine Zusammenarbeit mit dem Bereich «Digitale Transformation und IKT-Lenkung» (DTI) des Bundes initiiert. Vonseiten des Bundes ist das Interesse an der Datenföderation in Zusammenhang mit dem Grossvorhaben Ökosystem DataHub des DTI zu verorten. Zwischen den beiden Grossvorhaben besteht hohe Ziel- und Methodenkongruenz mit entsprechendem Synergiepotential. Zu den Modalitäten der Zusammenarbeit finden aktuell (mit Stand 10.01.2023) Gespräche statt.

2. Neue Datenparadigmen

Die Rolle, die Daten in der Gesellschaft spielen, und die Art und Weise, wie sie verwaltet werden, haben sich verändert. Daten sind nicht länger etwas, das gesammelt und zentral verwaltet wird. Stattdessen werden Daten zunehmend dezentral bereitgestellt und sowohl in strukturierten als auch unstrukturierten Formaten aggregiert. Um sie nutzen zu können - beispielsweise als Entscheidungsgrundlage - müssen sie entsprechend aufbereitet werden. Dies ermöglicht es zudem, Entscheidungen lokal durch mehrere Parteien zu treffen, ohne auf die Vermittlung einer zentralen Koordinationseinheit angewiesen zu sein. Daten werden auch immer häufiger für Rückschlüsse oder Prognosen verwendet. Dies bedeutet, dass Daten nicht nur für das Erstellen von Berichten, sondern auch in Echtzeit verwendet werden. Hier gelten neue Paradigmen der Datenverwaltung. Diese neuen Ansätze erfordern eine Architektur, die Innovationspotenzial bietet und das Experimentieren ermöglicht (z. B. Bildung von Datensätzen um datenanalytische Ansätze zu testen).

In Anbetracht der steigenden Anzahl an Produzentinnen und Produzenten sowie Konsumentinnen und Konsumenten von Daten wie auch der zunehmenden Vielfalt ihrer Datenverarbeitungsbedürfnisse ist eine zentralisierte Datenverwaltung mit Zuschnitt auf die Bedürfnisse einer Minderheit der Akteure immer weniger zu rechtfertigen. In einer zunehmend

dezentralisierten digitalen Welt erhalten geteilte Verantwortung und polyzentrische Governance eine bedeutendere Rolle. Diese Entwicklungen stellen die Ansicht in Frage, dass Governance entweder ein einheitlich definierter Prozess ist oder in den Zuständigkeitsbereich einer einzigen zentralen Behörde (einzentrische Governance) fällt. Vielmehr werden Entscheide von verschiedenen gemeinsam Akteuren getroffen, die Zugang zu unterschiedlichen Datenquellen benötigen. Es kommt hinzu, dass die Bestimmungen des neuen Datenschutzgesetzes deutlich strengere Kontrollen für die Erhebung, Bearbeitung, Aufbewahrung und Löschung von Daten vorsehen. Das neue Datenschutzgesetz setzt die Institutionen weiter unter Druck, ihre Daten sorgfältig zu verwalten. Dazu zählen neben der Datensparsamkeit auch eine verstärkte individuelle Selbstbestimmung. Beides ist mit bestehenden Lösungen nur schwer umzusetzen. Es entstehen somit neue Verpflichtungen und Haftungen, die Veränderungen seitens der Berufsbildung notwendig machen.

2.1 Blick auf das neue Datenschutzgesetz

Das neue Datenschutzgesetz (nDSG), das am 1. September 2023 in Kraft treten wird, bringt neue Herausforderungen für Datenverarbeiter und Datenverarbeiterinnen mit sich. Sowohl der öffentliche Sektor als auch der Privatsektor müssen sich darauf vorbereiten. Die Revision zielt insbesondere darauf ab, die informationelle Selbstbestimmung und die Privatsphäre der betroffenen Personen zu stärken. Es bezieht sich nur auf die natürlichen Personen, deren Daten verarbeitet werden. Die Revision festigt somit die Rechte der betroffenen Personen und erweitert parallel dazu die Pflichten der für die Verarbeitung verantwortlichen Personen. Dabei wird stets zwischen dem Status eines Bundesorgans und einer Privatperson unterschieden. Die für die Datenverarbeitung Verantwortlichen müssen die Einführung neuer Pflichten vorwegnehmen, insbesondere durch neue organisatorische und technische Massnahmen. Es obliegt den Datenverantwortlichen, insbesondere den öffentlichen Organen, die Rechte der betroffenen Person zu schützen. Sie müssen die Risiken auf der Grundlage einer Folgenabschätzung identifizieren und gleichzeitig die Datensicherheit gewährleisten, um die Vertraulichkeit, Verfügbarkeit, Integrität und Rückverfolgbarkeit der Daten sicherzustellen. Digitale Projekte müssen nach den Grundsätzen «Privacy by Design» und «Privacy by Default» gestaltet werden. Mit anderen Worten: Die für die Datenverarbeitung verantwortliche Person muss den Datenschutz bereits bei der Konzeption standardisiert einführen.

Um die Transparenz der Verarbeitung zu gewährleisten, wurde der Artikel über das Auskunftsrecht aktualisiert und stärkt dadurch die Informationspflicht. Der neue Artikel listet eine Reihe von zusätzlichen Informationen auf, die der betroffenen Person mitgeteilt werden müssen, wenn sie von ihrem Auskunftsrecht Gebrauch macht. Darunter fällt z. B. auch die Dauer der Speicherung personenbezogener Daten. Das nDSG enthält auch neue Begriffe wie Profiling und automatisierte Einzelentscheidungen, die mit Pflichten, wie der Informationspflicht, verbunden sind. Das Profiling durch ein Bundesorgan beispielsweise setzt die ausdrückliche Zustimmung der betroffenen Person voraus. Die Datenverantwortlichen müssen zudem ein Register führen, in dem alle Verarbeitungstätigkeiten aufgelistet sind. Bundesorgane müssen dieses Register zudem dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) übermitteln. Ebenso werden die Datenverantwortlichen verpflichtet, Fälle von Verletzungen der Datensicherheit zu melden, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person darstellen. Die

Datenverantwortlichen können freiwillig für Privatpersonen bzw. müssen obligatorisch für Bundesorgane einen Datenschutzberater oder eine Datenschutzberaterin ernennen. Schliesslich erweitert das nDSG die Strafbestimmungen, insbesondere die Verletzung der Geheimhaltungspflicht, indem es die Bussen auf bis zu CHF 250'000 festlegt.

2.2 Personenbezogene Daten: Wo sind diese in der Architektur der Datenföderation?

Grundlegend bei der Konzeption einer Datenföderation ist, dass der künftige Datenaustausch unter Einhaltung des Gesetzes geschieht. Die Rechte und Pflichten des neuen Datenschutzgesetzes lassen sich in der Architektur der Datenföderation verankern. Insbesondere von Interesse ist die Verortung von personenbezogenen Daten. Die im ersten Teil vorgestellte Architektur berücksichtigt die Grundsätze «Privacy by Design» und «Privacy by Default». Diese Grundsätze widerspiegeln die im nDSG verankerten Sorgfaltspflichten. Sie verpflichten die für die Datenverarbeitung verantwortlichen Personen, die notwendigen technischen Massnahmen zu ergreifen, um den Schutz der Daten zu gewährleisten und sie zu sichern.

Bevor der Datenlebenszyklus im Konzept der Datenföderation im Einzelnen erläutert wird, ist es wichtig, die folgenden Punkte festzuhalten:

- Das dezentrale Datenregister enthält keine personenbezogenen Daten.
- Nur autorisierte Akteure können auf das dezentrale Datenregister schreiben (es handelt sich um eine öffentliche und autorisierte Blockchain).
- Die Kommunikation zwischen den Parteien findet über eine direkte und verschlüsselte Verbindung statt.
- Jeder Akteur (Ausgabestelle, Inhaber:in, Prüfer:in) ist dafür verantwortlich, dass die Daten geschützt werden, die im Controller, Agenten oder der elektronischen Brieftasche verarbeitetet, weitergegeben oder gespeichert werden.

Im vorliegenden Konzept werden die Daten durch folgende Stellen bearbeitet:

- Nutzerin resp. Nutzer (Ausgabestelle, Inhaber:in, Prüfer:in): Sobald sie resp. er Daten an den Controller übermittelt oder durch den Controller Daten einsieht.
- Controller: Sobald er Daten von der Nutzerin resp. dem Nutzer an den Agenten und vom Agenten an die Nutzerin oder an den Nutzer weitergibt.
- Agent: Sobald er Daten z. B. generiert, sammelt oder weitergibt.
- elektronische Brieftasche: Sobald sie Daten aufbewahrt.

Die drei letzten Akteure können lokal oder in einer Cloud gespeichert werden. Die Wahl z. B. eines Cloud-Agenten bedeutet, dass die üblichen rechtlichen Fragen in Zusammenhang mit einer Cloud analysiert werden müssen, insbesondere jene in Bezug auf die Konformität der Datenverarbeitung.

Die Datenübertragung setzt den Aufbau eines Vertrauensverhältnisses, also eine direkte, verschlüsselte Verbindung, voraus. Diese wird durch einen privaten und einen öffentlichen Schlüssel ermöglicht, die von jedem Agenten generiert werden kann. Zwischen den Agenten wird nur der öffentliche Schlüssel ausgetauscht. Ohne diese Verbindung können die Akteure nicht miteinander kommunizieren. Die in diesem Dokument enthaltenen Daten sind beziehungsspezifisch, erneuerbar, zugänglich und nur den Parteien des Vertrauensverhältnisses

bekannt. Diese Peer-to-Peer-Vertrauensbeziehung ermöglicht es, die Vertraulichkeit, Verfügbarkeit, Integrität, aber auch die Nachvollziehbarkeit der übermittelten Daten zu gewährleisten.

Die übermittelten Daten befinden sich in den digitalen Nachweisen. Der Inhalt eines digitalen Nachweises hängt von der Art der Daten ab, die das Schema erfordert. Schemata enthalten keine personenbezogenen Daten, sondern geben – ähnlich wie ein leeres Formular – an, welche Art von personenbezogenen Daten eingegeben werden müssen. Schemata werden von autorisierten Personen (Mitgliedern der Datenföderation) erstellt und im dezentralen Datenregister hinterlegt. Die Schemata stellen sicher, dass die Grundsätze der Verhältnismässigkeit und der Datensparsamkeit eingehalten werden, indem die Daten standardisiert und auf das notwendige Minimum beschränkt werden. Die personenbezogenen Daten werden dann von der Ausgabestelle an ihren Controller gemeldet und von diesem an den Agenten weitergeleitet, damit ein digitaler Nachweis erstellt werden kann. Wie sensibel die in einem digitalen Nachweis enthaltenen Daten sind, hängt davon ab, welche Daten gemäss dem Schema erfasst werden müssen. Bei der Übermittlung eines digitalen Nachweises werden die personenbezogenen Daten vom empfangenden Agenten entschlüsselt, in der elektronischen Brieftasche aufbewahrt und vom Controller an die Empfängerin oder den Empfänger übermittelt. Im dezentralen Datenregister werden dabei keine personenbezogenen Daten gespeichert. Zu diesem Zeitpunkt kennen nur die Inhaberin bzw. der Inhaber und die Ausgabestelle den Inhalt des digitalen Nachweises.

Die Inhaberin oder der Inhaber eines digitalen Nachweises kann diesen wiederum in Form eines digitalen Dossiers an eine andere Person weitergeben, nachdem eine direkte und verschlüsselte Verbindung aufgebaut wurde. Die Prüfungsinstanz hat die Möglichkeit, die Echtheit des digitalen Nachweises zu überprüfen, indem sie den öffentlichen Schlüssel der auf dem digitalen Nachweis der Ausgabestelle mit dem im dezentralen Datenregister gespeicherten Schlüssel vergleicht. Dieser dezentrale öffentliche Identifikator bezieht sich nur auf eine Ausgabestelle. Es handelt sich daher nicht, um personenbezogene Daten im Sinne des nDSG.

Dank der Architektur und insbesondere der verschiedenen Strategien, die im nächsten Kapitel vorgestellt werden, ermöglicht das Konzept der Datenföderation den für die Datenverarbeitung verantwortlichen Personen, ihre Effizienz zu steigern und das nDSG einzuhalten, beispielsweise durch die Vermeidung toxischer Daten. Es ermöglicht auch, die Rechte der betroffenen Person zu stärken, indem es ihnen mehr Kontrolle über ihre Daten gibt.

2.3 Bewältigungsstrategien für den rechtskonformen Umgang mit toxischen Daten

Aufgrund der Architektur der Datenföderation für eine Berufsbildung können Daten effizienter und sicherer ausgetauscht werden. Das folgende Kapitel zeigt Strategien auf, wie in der Datenföderation Daten rechtskonform ausgetauscht werden können und nach welchen Grundsätzen dies geschieht.

Unter toxischen Daten werden personenbezogene Daten verstanden, die im weitesten Sinne des Wortes – willentlich oder unwillentlich – unrechtmässig bearbeitet wurden. Beispiele für die Entstehung von toxischen Daten sind Datenbearbeitungen, die:

- ohne Einwilligung oder ausreichende Rechtsgrundlage geschehen (z. B. unerlaubte Datenweitergabe);
- über den erforderlichen Zweck hinausgehen (z. B. Datenhortung);
- eine gesetzliche Frist überschreiten (z. B. verpasste Datenarchivierung).

Wie das letzte Beispiel verdeutlicht, kann die unrechtmässige Datenbearbeitung somit auch dazu führen, dass vormals rechtmässig bearbeitete Daten über die Zeit hinweg toxisch werden.

Wenngleich die Problematik toxischer Daten nicht auf die Berufsbildung beschränkt ist, so spielt sie ebenda eine wichtige Rolle. Erstens, da Personendaten der Lernenden verteilt bei den Kantonen (Schulort-, Lehrort-, Prüfungskantone), den Berufsfachschulen, den Organisationen der Arbeitswelt (OdA), den Lehrbetrieben, oder den Chefexpertinnen und Chefexperten liegen. Da die Strukturen dieser Akteure sehr heterogen sind, sind auch die von ihnen umgesetzten Datenschutzmassnahmen und die Art ihrer Datenverarbeitung sehr unterschiedlich. Zweitens, sind in der Berufsbildung bei der Datenverarbeitung eine Vielzahl von gesetzlichen Fristen einzuhalten, damit Daten nicht toxisch werden.

Insbesondere für kleine Lehrbetriebe, Berufsfachschulen oder OdA stellen die wachsenden Ansprüche an die Datenbearbeitung eine Herausforderung dar. Darüber hinaus wird die Thematik der toxischen Daten mit dem neuen Datenschutzgesetz weiter an Relevanz gewinnen (s. Kapitel 2.1). Die in Teil I des Konzepts (November 2022) beschriebene Datenföderation fokussiert daher auch auf die Vermeidung toxischer Daten. Zum einen geschieht dies bereits auf Ebene der Architektur durch den Grundsatz «Privacy by Design» (s Kapitel 2.2). Zum anderen eröffnet die Datenföderation den Akteuren Bewältigungsstrategien, die das Auftreten toxischer Daten verhindern oder stark reduzieren.

Die vielversprechendsten proaktiven Bewältigungsstrategien zur Vermeidung von toxischen Daten, die in einer Datenföderation in der Berufsbildung zum Einsatz kommen, werden in Tabelle 1 detailliert diskutiert. Dabei werden auch Vorteile für alle Akteure des Berufsbildungssystems aufgezeigt und eine rechtliche Einschätzung vorgenommen. Betreffend die beschriebenen Bewältigungsstrategien sind zwei Punkte wichtig zu bemerken:

Während die Architektur dem Entstehen toxischer Daten systemweit entgegenwirkt, müssen die in Tabelle 1 beschriebenen Bewältigungsstrategien von den einzelnen Akteuren implementiert werden, um der Problematik toxischer Daten entgegenzuwirken.

Ein zentrales Muster der Bewältigungsstrategien heisst «Automatisierung von Prozessen» (s. Box 1). Kurz: Für die Mitglieder einer Datenföderation geht die Verhinderung toxischer Daten auch mit einem Effizienzgewinn beim Datenaustausch einher.

Tabelle 1 : Ausgewählte Strategien zur Verhinderung von toxischen Daten, mögliche Vorteile und rechtliche Einschätzungen

N°	Bewältigungsstrategie	Beispiele	Rechtliche Einschätzung	Vorteile für Mitglieder	Vorteile für Teilnehmende
1	**Datensparsame Schemata:** Zur präventiven Vermeidung toxischer Daten werden Schemata so ausgestaltet, dass so wenig Daten wie notwendig in einem digitalen Nachweis erfasst (und ausgetauscht) werden.	Anmeldung einer Lernenden zum überbetrieblichen Kurs werden mithilfe eines digitalen Nachweises vorgenommen. Das berufsspezifische Schema ist so ausgestaltet, dass nur die notwendigsten Daten an die betreffende OdA übermittelt wird. Daten, die für die Anmeldung zum überbetrieblichen Kurs nicht zwingend notwendig sind, werden mithilfe des Schemas von der Übermittlung ausgenommen.	Die Schemas sind auf dem dezentralen Datenregister gespeichert (ohne Personendaten). Die Schemas verstärken den Grundsatz der Verhältnismässigkeit, indem Daten standardisiert werden und sie auf ein Minimum reduzieren.	*Autor:innen von Schemata*: Können in Schemata festhalten, welche Daten andere Akteure teilen dürfen. So kann ein Berufsbildungsamt z. B. ein Schema erstellen, das primär zum Datenaustausch zwischen Lehrbetrieben und OdA genutzt wird. *Ausgabestelle*: Befolgung des Grundsatzes der Datensparsamkeit reduziert mögliche Konsequenzen toxischer Daten. *Überprüfer:in*: Minimierung der Daten, die potenziell toxisch werden könnten (weil gar nicht erst übermittelt).	*Inhaber:in*: Garantie, dass nur so viel Daten erhoben werden, wie für einen bestimmten Zweck zwingend notwendig sind.

2	**Nutzungsbestimmungen** werden von der Ausgabestelle oder der Inhaber:in definiert und können Regeln darüber enthalten, was ein anderes Mitglied in der Datenföderation mit den Daten i) machen muss, ii) machen darf, oder iii) nicht machen darf. Nutzungsbedingungen werden einerseits verwendet um rechtliche Bestimmungen durchzusetzen und diese automatisiert auszulesen, andererseits können, wo das Gesetz dies zulässt, individuelle Regeln für den Umgang mit den eigenen Daten bestimmt werden.	Die Semesterzeugnisse einer Berufsfachschule (Ausgabestelle) werden als digitale Nachweise vergeben. Die Nutzungsbedingungen der Ausgabestelle beinhalten die gesetzlichen Aufbewahrungsfristen für die Ausgabestelle und die Überprüfer:in (z. B. ein Berufsbildungsamt). Eine Lernende definiert bei der Weitergabe des Semesterzeugnisses an Dritte (z. B. im Rahmen einer Bewerbung) eigene Nutzungsbedingungen (innerhalb des geltenden rechtlichen Rahmens).	Durch die Datenübermittlung kann die für die Verarbeitung verantwortliche Person die Inhaber:in somit direkt über die Verarbeitung ihrer Daten informieren, z. B. über die Dauer der Speicherung (vgl. Informationspflicht im nDSG). Durch die Übermittlung von Daten stimmt betreffende Person der Verarbeitung ihrer Daten zu. Indem sie der Übermittlung ihrer Daten Nutzungsbedingungen beifügt, kann sie den Umfang ihrer Zustimmung zur Verarbeitung ihrer Daten klarstellen.	*Ausgabestelle*: Verankert mittels Nutzungsbedingungen gesetzliche Archivierungsfristen direkt im digitalen Nachweis und schafft dadurch Transparenz. *Ausgabestelle oder Überprüfer:in*: Lesen Nutzungsbestimmungen maschinell aus und automatisieren das Datenlebenszyklusmodell (z. B. zur Einhaltung gesetzlicher Fristen). Voraussetzung für die Vorteile von Nutzungsbedingungen ist, dass die Daten nur im Agenten verwaltet werden, oder die Fachapplikation entsprechend angepasst wird, dass sie Nutzungsbedingungen maschinell auslesen kann.	*Inhaber:in*: Werden Daten mit privaten Lernorten geteilt, können diese mit Nutzungsbestimmungen versehen werden, die dazu führen, dass Daten automatisch gelöscht werden. Dadurch wird Insbesondere bei Anschlusslösungen der Entstehung von toxischen Daten vorgebeugt (z. B. Nutzung von digitalen Nachweisen in Bewerbungen).

3	**Zero Knowledge Proof** (ZKP): Wo möglich werden Informationen mittels ZKP auf eine «wahr» oder «falsch» Aussage reduziert. Dadurch können Aussagen darüber gemacht werden, ob eine Information in einem digitalen Nachweis ein bestimmtes Kriterium erfüllt, ohne die tatsächliche Information preiszugeben.	Viele Lernende werden während der Berufslehre volljährig. Dadurch verändert sich auch die rechtliche Situation für alle Beteiligten. Ein ZKP kommt zur Anwendung um jeweils die Volljährigkeit (nicht das genaue Geburtsdatum) zu prüfen, sei dies im Zusammenhang mit der Unterschrift von Absenzen in der Berufsfachschule, der Auskunft gegenüber Eltern durch die Berufsbildner:in, oder bei einer Änderung des Lehrvertrages.	Der ZKP-Algorithmus ermöglicht der Inhaber:in den Umfang und den Detaillierungsgrad der Daten, die an die Empfänger:in übermittelt werden, auf ein notwendiges Minimum zu begrenzen. Die Inhaber:in erhält damit mehr Kontrolle über den Detaillierungsgrad der durch sie weitergegebenen Daten. Die Empfänger:in erhält nur die Daten, die für den Abschluss eines Vorgangs notwendig sind.	*Ausgabestelle*: Mittels des datensparenden ZKP wird die Identität einer Ausgabestelle selbst bei der Verifizierung eines digitalen Nachweises durch die Überprüfer:in, geheim gehalten. Dies erlaubt es Ausgabestellen, ihr Amts- oder Berufsgeheimnis zu wahren, wo dies notwendig ist.	*Inhaber:in*: Wo möglich werden Informationen mittels ZKP auf eine Wahr- / Falsch-Aussage verkürzt, was es der Inhaber:in erlaubt, Informationen über sich auf datensparsame Art und Weise weiterzugeben. Korrelationsschutz bei Widerruf: *Überprüfer:in* kann kein Profiling betreiben
4	**Datensparsame digitale Dossiers**: Beim Zusammenstellen oder Abfragen eines digitalen Dossiers aus einem oder mehreren digitalen Nachweisen, werden nur jene Informationen ausgewählt, die für eine Entscheidfindung zwingend notwendig sind. Wie datensparsam ein Dossier ausgestaltet werden kann, ist abhängig von den geltenden Rechtsgrundlagen.	Beim Bewerbungsprozess nach Abschluss der Berufslehre wird nur die Abschlussnote geteilt, ohne die restlichen Zeugnisinformationen offen zu legen. Auch weitere Informationen können auf einfache Art und Weise vorenthalten werden, z. B., wenn die potenzielle Arbeitgeber:in in einem ersten Schritt den Namen und das Geschlecht der Bewerber:in noch nicht wissen will.	Die selektive Kommunikation stärkt das Prinzip der informationellen Selbstbestimmung. Die Inhaber:in hat damit die Möglichkeit, nur das zur Datenverarbeitung notwendige Minimum an Informationen zu teilen.	*Überprüfer:in*: Effizienzsteigerung durch gezieltere Abfragen. Für die Entscheidungsfindung werden nur die nötigen Informationen eines Lernenden abgefragt. Dadurch können Prozesse schlanker gestaltet werde. *Überprüfer:in*: Die Gefahr toxischer Daten ist stark reduziert, da die Menge an Daten, die durch ein datensparsames Dossier zur Überprüfer:in gelangen von Beginn weg deutlich eingeschränkt ist.	*Inhaber:in* entscheidet, in Situationen, wo das Recht nichts anderes vorsieht, selbst welche Daten geteilt werden.

2.4 Anwendungsfall: Ämter und Lernorte im Umgang mit Daten nach einem Lehrabbruch

Der untenstehende Anwendungsfall verdeutlicht, dass die Datenföderation nebst den in Tabelle 1 proaktiven Strategien auch reaktive Strategien im Umgang mit toxischen Daten ermöglicht, z. B. den Widerruf digitaler Nachweise. Auch diese Strategie beachtet die Grundsätze der Verhältnis- und Zweckmässigkeit sowie der informationellen Selbstbestimmung und ist gesetzeskonform. Mitglieder und Teilnehmende der Datenföderation werden rasch und unkompliziert über ein Ereignis informiert. Zentral ist dabei, dass die Prozesse aufgrund eines Ereignisses im System automatisch ausgelöst wird und Folgeprozesse bei den betreffenden Akteuren ausgelöst werden können.

Ämter und Lernorte im Umgang mit Daten nach einem Lehrabbruch

Das Berufsbildungsamt des Kantons Quantus – ein Kanton im Mittelland – hat gerade durch die Datenföderation erfahren, dass der Lernende Alex seine kaufmännische Lehre abgebrochen hat, da ihm diese Lehre inhaltlich nicht gefiel. Wie Abbildung 1 zeigt, fielen während Alex' erstem Lehrjahr an verschiedenen Orten des Berufsbildungssystems Daten über ihn an.

Aufgrund seiner Lehrvertragsauflösung müssen diese Daten nun unter Berücksichtigung der gesetzlichen Vorgaben, bearbeitet werden, damit sie nicht toxisch werden. Da Alex keinen Überblick hat, wo und wie seine Daten gespeichert sind, fühlt er sich der Kontrolle über seine Daten entzogen. Er beschliesst daher kurzerhand, alle seine bereits erstellten digitalen Nachweise zu widerrufen. Diese Transaktion löst Benachrichtigungen aus, welche alle relevanten Akteure in der Berufsbildung über ihren jeweiligen Handlungsbedarf bezüglich Alex' Daten informieren. Bei der Berufsfachschule und dem Berufsbildungsamt lösen die Transaktionen den jeweils vorgegebenen Archivierungsprozess aus, wodurch seine Daten nicht mehr als laufendes Dossier gehandhabt werden. Alex' ehemaliger Lehrbetrieb nimmt ebenfalls Kenntnis von dieser Meldung und leitet bei sich die jeweils notwendigen Schritte ein, d. h. die Löschung aller Daten, welche von Gesetzes wegen nicht mehr aufbewahrt werden dürfen. Auch die zuständige Organisation der Arbeitswelt, welche die ersten üK-Leistungen und weitere relevante Stammdaten über Alex besitzen, leiten die notwendigen Archivierungsprozesse ein. Zudem wird auch der Prüfungskommission gemeldet, dass Alex' Daten aufgrund der Lehrvertragsauflösung bearbeitet werden müssen. Selbst private Dienstanbieter (z. B. Anbieter von Einstufungstests oder private üK-Organisationen) könnten darüber in Kenntnis gesetzt werden, dass sie die Daten von Alex nach dessen Lehrvertragsauflösung entsprechend den gesetzlichen Vorgaben bearbeiten müssen. Schliesslich fliesst die Meldung über die Lehrvertragsauflösung von Alex – zwecks Bildungsmonitoring – pseudonymisiert in die kantonale Statistik beim Berufsbildungsamt ein.

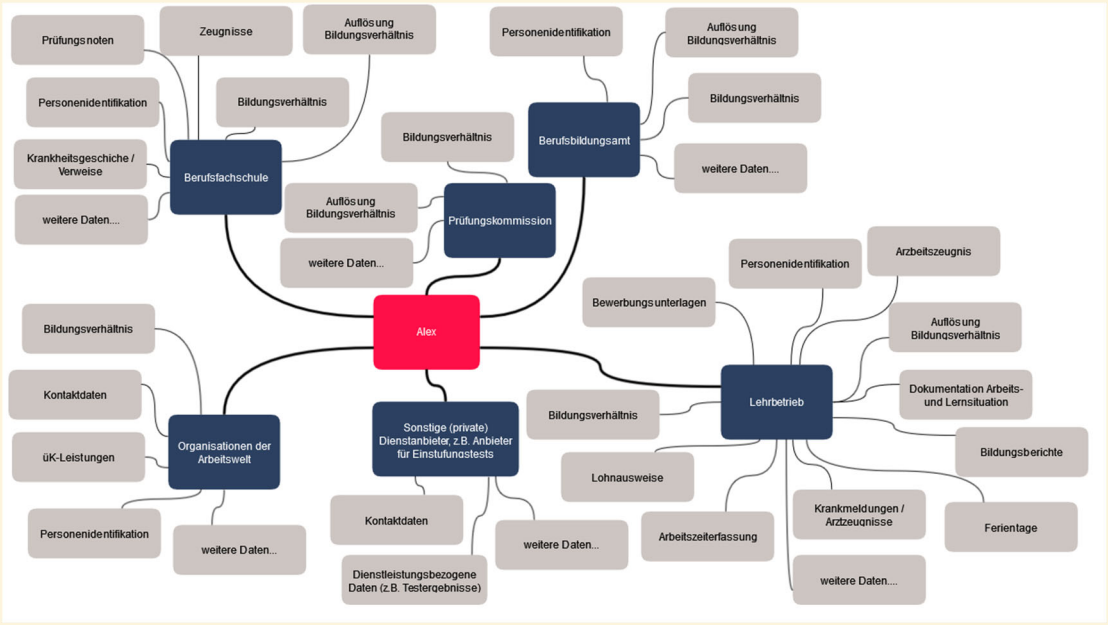

Abbildung 1 : Alex' Daten im Berufsbildungssystem zum Zeitpunkt einer Lehrvertragsauflösung

Hinweise: Die bei den jeweiligen Akteuren aufgeführten Daten sind beispielhaft und nicht abschliessend. Zudem ist es oft schwer nachzuvollziehen, welche Anzahl Attribute sich tatsächlich hinter einem Datenpunkt befindet. Der vorgeschlagene eCH-0260-Standard für den Datenaustausch in der Berufsbildung gibt hier einen guten Einblick über die Datenmenge, die mit einzelnen Meldungen verbunden sind (Text / Grafik).

3. Governance-Modell der Datenföderation

Eine Datenföderation ist ein gemeinsames Unterfangen verschiedener Organisationen (z. B. Berufsbildungsämter, Berufsfachschulen, Lehrbetriebe, Dienstleistungsanbieter etc.) mit jeweils eigenen Prioritäten und Interessen. Die berufliche Grundbildung verfügt über eine etablierte Governance (bspw. das Berufsbildungsgesetz, Gremien und Organe etc.). Für die Datenföderation braucht es eine Präzisierung der bestehenden Governance. Dies geschieht mittels eines Data-Governance-Modells. Dieses legt fest, wie der Datenaustausch zu organisieren ist und wie man am besten mit Problemen umgeht. Es beschreibt, wie Mitgliederorganisationen ihre Daten verwalten, austauschen und nutzen. Somit umfasst es Regeln, Richtlinien, Prozesse und Systeme für die Erfassung, Speicherung, Auswertung, Archivierung, Weitergabe und Löschung von Daten sowie Normen zur Gewährleistung der Sicherheit und Qualität dieser Daten. Das Ziel des Data-Governance-Modells ist es, allen beteiligten Akteuren der Datenföderation eine kohärente, effektive Nutzung und einen sicheren Austausch von Daten zu ermöglichen. So kann sichergestellt werden, dass die Daten einheitlich und verantwortungsvoll genutzt und die Rechte und Interessen aller Beteiligten geschützt werden. Die Einhaltung und Durchsetzung dieser Governance wird durch technische und organisatorische Vorkehrungen der Dateninfrastruktur ermöglicht. Das Data-Governance-Modell ist

somit das Instrument, mit dem die im ersten Teil dargelegten Architekturprinzipien in konkrete Handlungen umgesetzt werden können.

Zu diesem Zweck werden die folgenden Datendomänen unterschieden, die durch das Governance-Modell gesteuert werden:

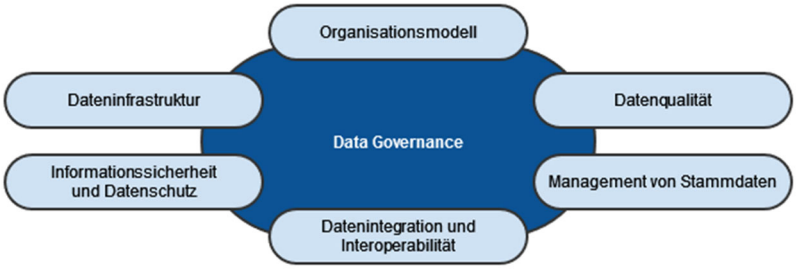

Abbildung 2 :Datendomänen des Data-Governance-Modells

Jeder Domäne beschreibt Standards und Praktiken, die in Kombination mit anderen Domänen zur Entwicklung von Problemlösungsstrategien genutzt werden können. So kann beispielsweise das Problem der Datenduplizierung in der Berufsbildung angegangen werden, indem sichergestellt wird, dass die Daten nur aus autoritativen Quellen stammen (Datenqualität), die mittels Peer-to-Peer Netzwerke direkt zugänglich gemacht werden (Dateninfrastruktur) und vordefinierte Standards verwenden (Datenintegration und Interoperabilität). Die jeweiligen Begrifflichkeiten werden untenstehend kurz erläutert und in den folgenden Kapiteln näher vorgestellt:

- **Organisationsmodell**: Die Definition von Rollen und Zuständigkeiten, Entscheidungsbefugnis und Delegation von Autorität, einschliesslich aller Formen von Instrumenten zur Durchsetzung dieser Vereinbarungen (z. B. Verträge) (s. Kapitel 3.1).
- **Dateninfrastruktur**: Die Gesamtheit aller Prozesse, Anwendungen und Datenbanken sowie die zugrunde liegenden Infrastrukturen, die erforderlich sind, um die Zielerreichung der Datenföderation zu gewährleisten (s. Kapitel 3.2).
- **Management von Stammdaten**: Die Definition der wichtigsten autoritativen Datenquellen innerhalb der Berufsbildung und die Bestimmung der Zugangsmethoden (inkl. Discovery). Solche Daten gelten somit standardmässig als richtig. Sie werden ohne weitere Prüfung übernommen und verwendet (s. Kapitel 3.3).
- **Datenqualität**: Die Domäne beinhaltet die Frage, wie die Datenqualität definiert und durchgesetzt wird, einschliesslich geeigneter Massnahmen zur Rechenschaftslegung über die Datenqualität (s. Kapitel 3.4).
- **Informationssicherheit und Datenschutz**: Technische und organisatorische Massnahmen zur Gewährleistung der Sicherheit und Integrität der Daten sowie des Schutzes der Rechte und Freiheiten von Personen durch geeignete Vorkehrungen zum Schutz ihrer personenbezogenen Daten (s. Kapitel 3.5).
- **Datenintegration und Interoperabilität**: Alle Normen (z. B. W3C, eCH etc.) und damit zusammenhängenden Bestimmungen, die den Datenaustausch sicherstellen. Dabei muss eine angemessene Integration von Daten in Drittsysteme und Interoperabilität derselben

zwischen Produzentinnen und Produzenten sowie Konsumentinnen und Konsumenten gewährleistet werden (s. Kapitel 3.6).

Das Data-Governance-Modell stellt sicher, dass die Datenföderation durch die Regelung der geteilten Verantwortung im Interesse seiner Mitglieder handelt. Dies wiederum gewährleistet die Rechenschaftspflicht und Rückverfolgbarkeit der Handlungen in einem verteilten und dezentralen System. Die Transparenz der Dateninfrastruktur (z. B. dezentrales Datenregister und dessen Transaktionen) erhöht das Vertrauen und verringert systemische Risiken (z. B. Datenschutz). Ausserdem werden durch die Art der Datenübermittlung die Latenzzeiten verkürzt, was zu einer schnelleren Entscheidungsfindung führt und gleichzeitig die Partizipation verbessert. Im folgenden Abschnitt wird das Data-Governance-Modell ausführlicher beschrieben.

3.1 Organisationsmodell: Rollen und Instrumente in der Datenföderation

Für das das Data-Governance-Modell in der Datenföderation werden folgende Rollen unterschieden:

- **Mitglieder** sind beteiligte Organisationen, die in der Datenföderation vertraglich gebunden sind. Sie stellen Dienste bereit und interagieren mit der zugrunde liegenden Infrastruktur (d. h. sie haben die Kontrolle über und die Verantwortung für ihre Agenten und deren Controller). Beispiele von Mitgliedern sind Berufsbildungsämter, Berufsfachschulen, Lehrbetriebe und andere Unternehmen, die bestehende oder neue Dienstleistungen anbieten.
- **Teilnehmende** sind Konsumentinnen oder Konsumenten, der von den Mitgliedern erbrachten Dienste. Sie haben (normalerweise) keine direkte Interaktion mit der zugrundeliegenden Infrastruktur, obwohl unter bestimmten Bedingungen Lesezugriff gestattet wird (z. B. zum Zweck der Validierung von digitalen Nachweisen). Beispiele von Teilnehmenden sind Lernende und deren Erziehungsberechtigte, die auf Daten in der Berufsbildung zugreifen oder Daten (via Dienste der Mitglieder) bereitstellen wollen.
- Der **Technische Betrieb** der Datenföderation ist für die technische Architekturvorgaben sowie deren Umsetzung, Pflege und Wartung zuständig. Dies geschieht unter Aufsicht der Geschäftsstelle und in Zusammenarbeit mit den Mitgliedern der Datenföderation (z. B. in dem sie Knoten hosten etc.).
- Die **Geschäftsstelle** der Datenföderation ist der administrative Dreh- und Angelpunkt, der für die Verwaltung der Datenföderation zuständig ist (z. B. Kommunikation, Betriebsprozesse, Vertragsmanagement etc.).
- Die **Bildungspolitische Steuerung** ist für die Governance, Strategie, Zielsetzung und Prioritätensetzung der Datenföderation zuständig. Darin sind alle wesentliche Mitgliedergruppen der Datenföderation (d. h. Berufsbildungsämter, Berufsfachschule, OdA etc.) vertreten.

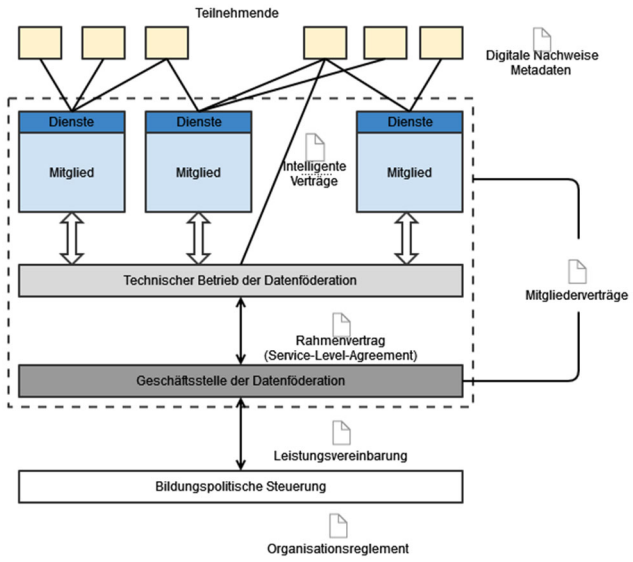

Abbildung 3 : Die Rollen im Verhältnis zu den Governance-Instrumenten

Die folgenden Governance-Instrumente werden eingesetzt:

- **Organisationsreglement**: Eine übergreifende Grundsatzerklärung in Bezug auf die Funktion der Datenföderation und die darin enthaltenen Rollen und Zuständigkeiten.
- **Leistungsvereinbarung**: Eine Konkretisierung der funktionalen Aufgaben der Geschäftsstelle im Rahmen der politisch beabsichtigen Ziele der Datenföderation. Diese Vereinbarung besteht zwischen der bildungspolitischen Steuerung und der Geschäftsstelle im Rahmen ihrer bestehenden Funktion.
- **Rahmenvertrag** (Service-Level-Agreement): Ein Instrument zur Definition der erwarteten Leistung und anderer nicht-funktionaler Merkmale (z. B. Sicherheit, Skalierbarkeit, Verfügbarkeit etc.). Dabei handelt es sich um einen Vertrag zwischen der Geschäftsstelle und dem technischen Betrieb.
- **Mitgliederverträge**: Die Mitgliedschaft bei der Datenföderation unterliegt Verträgen, die von der Geschäftsstelle bereitgestellt werden. Teilnehmende haben dagegen keine (schriftliche) Vertragsbeziehung zur Datenföderation.
- **Metadaten digitaler Nachweise**: Alle Metadaten, die zur Regelung der Verwendung von digitalen Berechtigungsnachweisen dienen (z. B. Nutzungsbedingungen, die Berechtigungen, Verbote und Verpflichtungen regeln).
- **Intelligente Verträge** (Smart Contracts): Spezifische algorithmische Entscheidungen können mittels Softwareverträgen delegiert werden, die Aufträge auf der Grundlage von Transaktionsereignissen im dezentralen Datenregister ausführen. Diese Software kann wiederum Benachrichtigungen ausgeben, die von Mitgliedern (oder anderen Parteien) abonniert werden können. Diese Benachrichtigungen können von den Mitgliedern für weitergehende Handlungen genutzt werden.

3.2 Bedeutung einer Dateninfrastruktur für die Qualität und Effizienz des Bildungssystems

Die Schaffung einer Dateninfrastruktur, die die Struktur, die Standards und die Verwaltung der Daten des Bildungssystems umfasst, soll deren Qualität, Genauigkeit und Zuverlässigkeit gewährleisten. Sie hilft beispielsweise dabei, Verbesserungsmöglichkeiten in den Datenverwaltungsprozessen zu erkennen und so effizienter und kostengünstiger zu werden, aber auch die Qualität der Entscheidungsfindung zu verbessern. Dies kann durch einen stärkeren Einbezug derjenigen erreicht werden, die entscheidungsrelevante Daten liefern, wie auch durch die Befähigung jener Akteure, die an der Entscheidungsfindung mitwirken. Jene Befähigung entsteht durch die von der Dateninfrastruktur geschaffene strukturelle Gegebenheiten, welche die direkten Verbindungen zwischen Akteuren ermöglicht (z. B. Synchronität der Kommunikation, Transparenz der Transaktionen etc.).

Die Mitglieder der Datenföderation sind als Knoten (Nodes), Agenten und deren Controller ersichtlich (s. Abbildung 4). Sie sind vertraglich an gemeinsame Regeln für die Datenverarbeitung gebunden (einschliesslich Erstellen, Bereitstellen, Verwenden, Speichern und Löschen von Daten). Jene Verpflichtungen umfassen den Umgang mit technischen Komponenten (z. B. Agenten), inkl. deren Massnahmen zum Schutz der Datenföderation sowie die Einhaltung der Architekturvorgaben. Diese sind vom technischen Betrieb vorgegeben und wurden von der Geschäftsstelle genehmigt. Solche Verträge übertragen somit Rechte und Pflichten. Sie gewähren je nach Art der Mitgliedschaft bestimmte technische Berechtigungen (z. B. Schreibrechte oder Zugang auf bestimmte Daten etc.). In erster Linie wird hierdurch eine gemeinsame Verantwortung geschaffen, durch die Vertrauen aufgebaut wird. So werden z. B. durch den Beitrittsprozess die notwendigen Vertrauensmaterialen, wie beispielsweise öffentliche Schlüssel, institutionelle Informationen und sonstige Artefakte im dezentralen Datenregister hinterlegt.

Als technischer Betrieb fungiert diejenige Organisation, die für den Betrieb, die Wartung und Pflege der gemeinsamen Infrastruktur der Datenföderation verantwortlich ist. Teile dieser Verantwortung können an Mitgliederorganisationen delegiert werden, die die Vorgaben vom technischen Betrieb einzuhalten haben. Gemeinsame Komponenten wie Knoten und das dezentrale Datenregister werden nach einheitlichen Kriterien betrieben. Dies betrifft nicht nur die technischen Spezifikationen (z. B. die Verwendung von virtualisierten Containern für das Hosting von Software), sondern auch die Governance von Softwarekomponenten (d. h. Software-Architekturrichtlinien für die Erstellung von Intelligenten Verträgen sowie die Handhabung von deren Updates etc.). Aus diesem Grund stützt sich das Governance-Modell auf sogenannte «permissioned» Technologien bei denen die beteiligten Organisationen Mitwirkungsrechte haben, die auf dem bestehenden Vertrauen im Bildungswesen beruhen. Dies steht im Gegensatz zu anderen z.B. ökologisch problematischen Ansätzen, wie beispielsweise kostspielige Proof-of-Stake-Konsensalgorithmen, die sehr energieaufwendig sind (z. B. Bitcoin).

3.3 Management von Stammdaten

Stammdaten sind Daten, die für die Berufsbildung am wichtigsten sind und daher als kritisch gelten. Stammdaten umfassen nicht nur die Referenzdaten der Berufsbildung (wie beispielsweise institutionelle Informationen), sondern auch betrieblich wichtige Daten (z. B. Noten und sonstige Leistungsnachweise). Derzeit gibt es in der Berufsbildung kaum einen Konsens darüber, was genau Stammdaten sind und welche Geschäftsregeln angewandt werden müssen, um ihre Integrität zu wahren. Zahlreiche bestehende Dienste könnten dennoch Schnittstellen zu wichtigen Daten bilden, darunter das Lehrstellenregister (LSR) und damit verbundene Profession Services (inkl. Berufsregister). Diese Daten können mithilfe der Datenföderation von den entsprechenden offiziellen Quellen bezogen werden. In der Praxis ist es jedoch zurzeit schwierig, automatisch jene Quellen zu ermitteln und mit ihnen in Verbindung zu treten, so dass die Daten häufig mehrfach erfasst werden müssen (z. B. Wohnortsangaben). Dies führt zu Doppelspurigkeiten und Schwierigkeiten bei der Aktualisierung der Daten (z. B. bei Adressänderungen). Deshalb bietet die Datenföderation einen Informationsdienst (sogenannten Discovery-Service) an. Die angesprochenen Quellen müssen dabei nicht innerhalb das Bildungssystem verortet sein (z. B. Personenattribute aus einem E-ID-System, Wohnortsdaten bei einer Einwohnerkontrollstelle (EWK) etc.). Die Datenföderation schlägt eine sogenannte Registry-Architektur-Topologie vor, d. h. die Stammdaten sind an verschiedenen Orten verteilt, die aber im dezentralen Register indiziert sind.

Beispielsweise möchte ein Berufsbildungsamt (als Mitglied der Datenföderation) wissen, wie die korrekte Wohnortsadresse eines Lernenden lautet. Der Controller des Berufsbildungsamt erfährt automatisch durch seinen Agenten via den Discovery-Dienst aus welcher Quelle die Daten für diesen Lernenden zu erhalten sind (z. B. die EWK des Kantons) und setzt sich direkt damit in Kontakt. Die dafür nötige technische Referenzdaten sind im dezentralen Register hinterlegt (z. B. Art des Kontakts zum Service Point) und sind von der jeweiligen Quelle (z. B. EWK) zu verwalten. Der Austausch von Daten erfolgt mittels digitalen Nachweisen, die von der EWK digital signiert sind und direkt ans Berufsbildungsamt gesendet werden. Kommt es später zu einer Adressänderung, kann die EWK-Stelle das Berufsbildungsamt via Agent-Infrastruktur automatisch darüber informieren. Es ist wichtig zu beachten, dass keine abgefragten Daten innerhalb des dezentralen Datenregisters bearbeitet oder gespeichert werden.

Der Agent kann dann angewiesen werden, die benötigten Informationen direkt abzurufen und sie an den Controller zurück zu senden. Dies wird durch an den eCH-Standard angelehnte Protokolle und standardisierte Schnittstellen erreicht, die die Fachapplikationen (FA) zur Verfügung stellen. Die Datenföderation ermöglicht es, dass die entsprechenden Stellen durch das dezentrale Datenregister kontaktiert und die Daten verschlüsselt und sicher ausgetauscht werden. Die Controller dienen in diesem Fall als Schnittstelle zu den bestehenden Systemen. In manchen Fällen (z. B. E-ID, das Self Sovereign Identity (SSI) verwendet) sind keine Schnittstellen erforderlich. Die E-ID würde im selben Ökosystem existieren, so dass Daten direkt bei den Teilnehmenden abgefragt werden können.

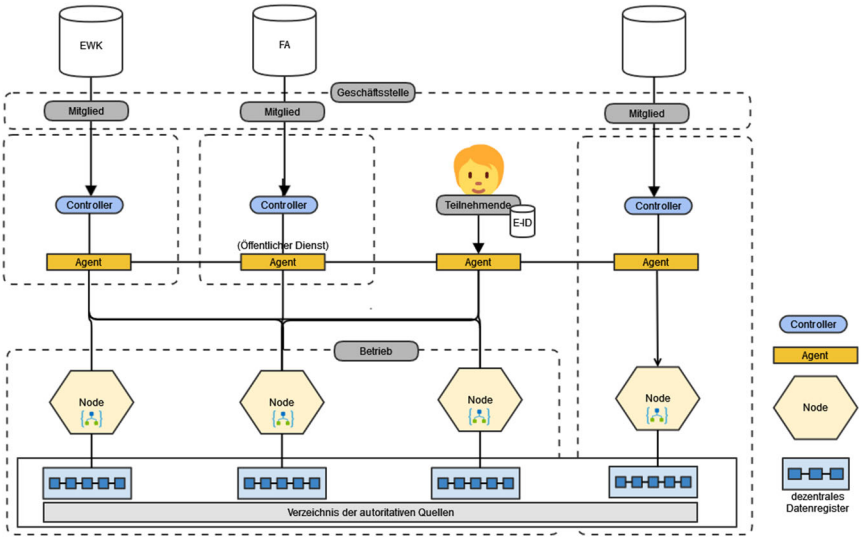

Abbildung 4 : Umgang mit Stammdaten (autoritative Quellen)

3.4 Datenqualität

Datenqualität ist zweckgebunden. Entsprechend ist die Definition von Datenqualität situativ festzulegen. Es ist die Aufgabe der Datenquellen in der Berufsbildung unter Berücksichtigung der Bedürfnisse aller Anspruchsgruppen eine angemessene Definition von Datenqualität, insbesondere unter Einbezug der entsprechenden eCH-Standards, festzulegen. Gewöhnlich bezieht sich eine solche Definition auf folgende Elemente:

- Aktualität: Daten entsprechen dem jeweils aktuellen Zustand der erfassten Realität.
- Eindeutigkeit: Es ist eindeutig interpretierbar, was mit den Daten erfasst wurde.
- Einheitlichkeit: Gleiche Tatsachen, werden gleich erfasst.
- Genauigkeit: Tatsachen werden hinreichend exakt erfasst.
- Konsistenz: Erfasste Daten sind in sich widerspruchsfrei.
- Korrektheit: Tatsachen werden realitätsgetreu erfasst.
- Redundanzfreiheit: Daten weisen keine Doubletten auf.
- Relevanz: Daten erfassen, mit den für einen Vorgang wichtigen und notwendigen Informationen.
- Verständlichkeit: Daten stimmen in ihrer Begrifflichkeit und Struktur mit den Kenntnissen der Nutzenden überein.
- Vollständigkeit: Daten sind weitgehend frei von fehlenden Werten.
- Zuverlässigkeit: Entstehung und Herkunft der Daten sind nachvollziehbar.

Für die Zwecke der Datenföderation werden Daten als von (akzeptabler) Qualität angesehen, wenn sie für die beabsichtigte Verwendung im Betrieb und bei der Entscheidungsfindung geeignet sind. In einer verteilten Umgebung wie die berufliche Grundbildung stellt dies eine erhebliche Anforderung an die Produzenten und Produzentinnen von Daten, die die Datennutzungsbedürfnisse durch (mehrere) Verbraucher antizipieren müssen. Aus diesem Grund wird

die Datenqualität als ein Service-Qualität-Kriterium betrachtet. Dieses wird über das dezentrale Register veröffentlicht und ermöglicht es den Datenkonsumentinnen und Datenkonsumenten, die für ihre Bedürfnisse am besten geeigneten Datenquellen mittels Informationsdienst auszuwählen. Wenn Agenten also mit dem dezentralen Datenregister interagieren, liegt die Verantwortung für die Richtigkeit von deren durchgeführten Operationen und Daten bei den jeweiligen Mitgliedern, die die Agenten betätigt haben.

Um Probleme mit der Aktualität der Datenqualität zu verringern (d. h. Daten, die zum Zeitpunkt der Erhebung korrekt waren, aber zum Zeitpunkt der Nutzung nicht mehr korrekt sind), ist es notwendig, möglichst direkte Wege zwischen den Akteuren der Berufsbildung zu schaffen (s. Kapitel 3.2). Dies bedeutet, dass die Zentralisierung der Daten vor deren Bearbeitung ein Risiko für die Datenqualität darstellt, welches aber durch die von der Datenföderation vorgeschlagene Architektur grösstenteils beseitigt wird. Die Aktualität und Rechtzeitigkeit von Daten spielt übrigens nicht immer eine Rolle für die Datenqualität wie beispielsweise bei der Forschung von historischen Daten.

Durch die Datenföderation kann die Datenqualität verbessert werden. Dies unter anderem wegen der Governance im gesamten Datenlebenszyklus (und somit der Rechenschaftspflicht) wie auch der Datenaktualität durch den direkten Austausch zwischen Produzentinnen und Produzenten sowie Konsumentinnen und Konsumenten. Zudem stützt sich die Datenföderation auf zuverlässige Quellen, die sich zur Einhaltung einer gemeinsamen Definition von Datenqualität verpflichtet haben und die Integrität der Daten sicherstellen. Dies geschieht im Sinne einer Datenprovenienz, d. h. die Rückverfolgbarkeit bestimmter Daten zu ihren ursprünglichen Quellen sowie insbesondere durch automatisierte Geschäftsregeln und Datenbank-Integritätsbedingungen. Darüber hinaus können Schemata für digitale Nachweise im dezentralen Datenregister gespeichert werden. Diese können zur Überprüfung der Konformität mit den Datenqualitätsstandards verwendet werden. Dadurch wird die Vertrauenswürdigkeit von Daten und somit die Wahrscheinlichkeit, dass die richtigen Daten für Entscheide verwendet werden, erhöht.

3.5 Informationssicherheit und Datenschutz

Die Datenföderation bietet neue Wege Daten auszutauschen und zu nutzen. Durch die Vermeidung zentraler Datenverarbeitungssilos wird sichergestellt, dass innerhalb des Bildungssystems weniger Klumpenrisiken bestehen. Damit können Risiken durch Cyberkriminalität erheblich reduziert werden. Die Daten werden von jenen Instanzen erhoben, bearbeitet und verteilt, die tatsächlich an der operativen Entscheidungsfindung beteiligt sind. Ein zentrales Element der Infrastruktur ist die Bereitstellung von Vertrauensmaterialien (z. B. öffentliche Schlüssel), die sich auf etablierte Bildungseinrichtungen beziehen und für die Zwecke der Validierung verwendet werden können. Dies ähnelt den klassischen hierarchischen Ansätzen im Internet (z. B. Public-Key-Infrastructures), ist jedoch dezentraler und daher leichter zu verwalten. Der daraus entstehende hohe Grad an Anschlussfähigkeit innerhalb des Netzes wird durch paarweise kryptografisch geschützte Vertrauensbeziehungen gesichert. Somit ist es nicht notwendig, das Vertrauen in Form einer klassischen Identitätsmanagement-Lösung zu zentralisieren, was wiederum das Risiko von Identitätsdiebstahl deutlich reduziert. Diese Massnahmen verringern die Risiken für Cyberangriffe, die versuchen den Datenaustausch

zwischen zwei Akteuren unbemerkt abzufangen, mitzulesen oder zu manipulieren. Die Dezentralisierung sorgt für eine höhere Resilienz und Ausfallsicherheit gegen gängige und teilweise bereits eingetretene Angriffsstrategien (z. B. Denial of Service, Ransomware etc.).

Die Datenföderation kann zudem auch spezifische Massnahmen ergreifen, um einen besseren Datenschutz zu gewährleisten. Der dezentrale Charakter des Netzes verbessert sowohl Zweckbindung als auch Datensparsamkeit. Dies liegt daran, dass die Daten weitgehend oder nur zwischen den teilnehmenden Akteuren ausgetauscht werden, ohne dass eine Zentralisierung in «datenhungrigen» Silos erforderlich ist. Dadurch werden die sekundären Risiken aggregierter Daten vermieden. Diese entstehen, wenn einzelne Elemente zwar auf legitime Weise erhoben werden, aber dennoch ein kollektives Risiko darstellen, wenn sie zusammen mit anderen Daten gespeichert werden. Innerhalb der Datenföderation sind gemeinsame Daten nur im dezentralen Datenregister zu finden. Diese Daten werden aber durch dezentrale Identifikatoren referenziert, die nur den betroffenen Parteien bekannt sind. Dadurch wird die Übermittlung von bildungsrelevanten Ereignissen ermöglicht, ohne die Preisgabe von den Parteien bisher unbekannten Informationen. Oft reicht es auch aus, Aussagen über Daten zu machen, ohne dass die Daten selbst offengelegt werden müssen. Dies ist insbesondere der Fall, wenn binäre Aussagen gemacht werden müssen (z. B. ob eine Lernende oder ein Lernender volljährig ist oder nicht). Hier ermöglicht der Zero-Knowledge-Proof-Ansatz, Aussagen in Form von kryptographischen «Beweisen» zu machen (z. B. die Volljährigkeit eines Lernenden ohne sein Geburtsdatum preiszugeben). Solche Dienste sind als integraler Bestandteil der Schnittstelle zur Datenföderation geplant.

Bei der Übermittlung von Daten kann dies in Form eines digitalen Nachweises geschehen, in dem Nutzungsbedingungen festgehalten werden können. So ist es zum Beispiel möglich, Nutzungsbedingungen zu definieren, die festlegen, was erlaubt oder verboten ist oder welche anderen Verpflichtungen gelten. Diese dienen als Beleg, mit dem die Datenbearbeiterin oder der Datenbearbeiter ihre bzw. seine Rechtspflichten ausüben und die Einhaltung des Datenschutzgesetzes bestätigen kann. Zudem bietet die Datenföderation einen Benachrichtigungsdienst, womit betroffene Parteien über einen eventuellen Widerruf eines bereits erstellten digitalen Nachweises informiert werden. Somit wird klar, wann und wo Handlungsbedarf besteht, ohne stets auf Applikationslogik angewiesen zu sein, deren Implementierung und Einspielen recht viel Zeit in Anspruch nehmen kann.

3.6 Datenintegration und Interoperabilität

Ziel der Datenföderation ist es den Prozess zur Kombination von Daten aus verschiedenen Quellen (z. B. von den drei Lernorten) zu erleichtern und zu vereinfachen. Die Integrierbarkeit unterschiedlicher Datenbestände in der Föderation beruht nicht nur auf der oben beschriebenen Infrastruktur, sondern auch durch die Einhaltung von Normen und die Einbindung bestehender Datenmanagementlösungen bei den Akteuren der beruflichen Grundbildung. Diese Normen sind inzwischen international standardisiert und bilden die Grundlage für die Interoperabilität. Sie fördern das Wachstum und die Integration jener Ökosysteme, die derzeit in der Schweiz und international (z. B. European Blockchain Services Infrastructure (EBSI)) entstehen. So wird es möglich, dass Lösungen im Bereich der Berufsbildung mit

denen anderer Branchen wie der eGov, digitalen Verwaltung und den Sozialdiensten kompatibel sind.

Der primäre Datenträger in solchen Ökosystemen – wie auch in dem vorliegenden Konzept der Datenföderation – ist der digitale Nachweis (wie in Teil I beschrieben). Dabei ist es möglich (und sinnvoll), dass mehrere ausstellende Institutionen ihre digitalen Nachweise (z. B. für Zeugnisse, Lehrstellenmeldungen oder Bildungsbewilligungen) auf Basis gemeinsam definierter Schemata erstellen. Da alle Vorlagen auf dem gemeinsamen, dezentralen Datenregister abgelegt sein müssen, erleichtert die vorgeschlagene Architektur die systemübergreifende Nutzung solcher Vorlagen erheblich. Für die Definition von Formaten in den Vorlagen wird auf bestehende Datenstandards zurückgegriffen, beispielsweise auf den eCH-0260 Datenstandard «Berufsbildung». Gemeinsam genutzte Schemata auf Basis bestehender Standards sichern so ein hohes Mass an Interoperabilität und damit die Fähigkeit, kantons- und institutionsübergreifend Daten austauschen zu können.

Der Rückgriff und die konsequente Umsetzung bestehender Datenstandards bilden darüber hinaus den Kern für die Einbindung bestehender Datenmanagementsystemen in die Föderation. Sie wird durch die Spezifikation von Schnittstellen zwischen Controllern und den bestehenden Datenbanklösungen der Mitglieder der Föderation sichergestellt. Es ist wichtig zu betonen, dass es in der vorgeschlagenen Architektur möglich bleibt, Informationen zwischen einzelnen Mitgliedern in nicht-standardisierter Form oder ohne Verwendung digitaler Nachweise auszutauschen (z. B. in Form von Meldungen oder anderen Interaktionen). Beispielsweise bleibt es möglich, dass im oben beschriebenen Anwendungsfall das Berufsbildungsamt den Lehrbetrieb, die Berufsfachschule und die üK-Anbieter über den Lehrabbruch eines Lernenden informiert. Dies kann in Form einer einfachen Nachricht geschehen. Durch die Nutzung kryptographisch gesicherter Peer-to-Peer-Kanäle ist diese Form des Austausches zudem bedeutend sicherer als beispielsweise ein Austausch via E-Mail.

4. Zwischenfazit

Der vorliegende zweite Teil des Konzepts zur Datenföderation für die Berufsbildung gibt einen Einblick in das Potenzial, der im ersten Teil beschriebenen technischen Architektur im Umgang mit den anstehenden datenschutzrechtlichen Herausforderungen. Mit der neuen Datenschutzgesetzgebung steht ein eigentlicher Paradigmenwechsel an: Dem Individuum werden künftig wesentlich weitreichendere Verfügungsrechte zugestanden. Die technische Architektur unterstützt Bewältigungsstrategien im Umgang mit personenbezogenen Daten.

Das für die künftige Datenföderation vorgeschlagene Data-Governance-Modell ist polyzentrisch konzipiert. In Anbetracht der steigenden Anzahl an Produzentinnen und Produzenten sowie Konsumentinnen und Konsumenten von Daten wie auch der zunehmenden Vielfalt ihrer Datenverarbeitungsbedürfnisse ist eine zentralisierte Datenverwaltung mit Zuschnitt auf die Bedürfnisse einer Minderheit der Akteure immer weniger zu rechtfertigen. In einer zunehmend dezentralisierten digitalen Welt spielen geteilte Verantwortung und verteilte Governance eine immer wichtigere Rolle. Das Data-Governance-Modell ist komplementär zur dezentralen technischen Architektur ausgelegt.

Das Konzept der Datenföderation für die Berufsbildung fügt sich in eine im Aufbau befindende Landschaft vertrauenswürdiger, föderal organisierter Datenräume ein. Es handelt sich um Datenräume, die national wie auch zunehmend international interoperabel ausgestaltet sind.

Anhang

Begrifflichkeiten

Begriff	Definition
Agent	Ein Agent ist eine Softwarekomponente, die die Anweisungen eines oder mehrerer Controller verarbeitet, entsprechend in der Datenföderation weiterverbreitet, mit den Knoten kommuniziert oder digitale Nachweise (und damit personenbezogene Daten) speichert.
Ausgabestelle	Unter einer Ausgabestelle («Issuer») versteht man eine Stelle, die z. B. durch eine staatliche Institution autorisiert ist, digitale Nachweise auszustellen.
Autoritative Quelle	Datenquellen, die ein hohes Mass an Glaubwürdigkeit und Vertrauen besitzen.
Betreiber:in	Dies können Institutionen, private oder juristische Personen sein, die Knoten betreiben.
Blockchain	Ein Ledger-Speichersystem, bei dem Transaktionsdaten angehängt werden und nicht nachträglich geändert werden dürfen. Blockchains werden durch ein Netzwerk von Knoten realisiert und sind daher in der Regel dezentralisiert.
Controller	Unter Controller versteht man eine Software-Komponente, die es Personen und Institutionen ermöglicht, über eine Benutzeroberfläche auf den Agenten zuzugreifen und so Zugang zu digitalen Nachweisen zu erhalten, das dezentrale Datenregister zu nutzen oder mit anderen Mitgliedern oder Teilnehmenden der Datenföderation zu kommunizieren.
Datenprovenienz	Die Rückverfolgbarkeit bestimmter Daten zu ihren ursprünglichen Quellen. Damit kann beispielsweise festgestellt werden, ob bestimmte Daten tatsächliche von autoritativen Quellen stammen.
Dezentrales Datenregister	Ein dezentrales Datenregister ist ein öffentlich zugänglicher und von allen lesbarer dezentraler Speicher, der alle notwendigen Informationen enthält, um eine Datenföderation im Allgemeinen und ein Ökosystem für digitale Nachweise im Speziellen betreiben zu können.
Dezentrale Identifikatoren (DID)	Eine Form der Identifikation, die in dezentralen Systemen verwendet wird und die Verknüpfung von Ereignissen mit Daten in einer Weise ermöglicht, dass nur die betroffenen Parteien jene Verknüpfungen herstellen können.
Elektronische Brieftasche	Bei einer elektronischen Brieftasche handelt es sich um eine Software-Applikation für die sichere Aufbewahrung digitaler Nachweise.
Informationsdienst (sog. Discovery-Service)	Ein technischer Dienst, der innerhalb des dezentralen Datenregisters die (automatische) Ermittlung von Dienstleistungen, die von Mitgliedern angeboten werden, ermöglicht.
Inhaber:in	Unter Inhaberin oder Inhaber versteht man die Person oder Institution, die einen digitalen Nachweis elektronisch besitzt.

Intelligente Verträge (Smart Contracts)	Intelligente Verträge sind Computerprogramme, die die automatisierte Bearbeitung von Daten und darauf basierend eine automatisierte Entscheidungsfindung entlang von vordefinierten Kriterien bewirken.
Knoten (Node)	Ein Knoten ist eine Verarbeitungsinstanz des dezentralen Datenregisters. Knoten tätigen, überprüfen und speichern Transaktionen auf dem dezentralen Datenregister und können zudem auch intelligente Verträge hosten.
Mitglied	Eine institutionelle Partei der Datenföderation, die aktiv mitwirken darf (z. B. Erstellen von Transaktionen). Solche Parteien müssen mit dem Betreiber der Datenföderation einen Vertrag unterzeichnen.
Nutzungsbedingungen	Metadaten, die auf digitalen Nachweisen zum Zwecke der Regelung der Berechtigungen, Verbote und Verpflichtungen geschrieben werden.
Permissioned (Blockchain)	Eine Blockchain Infrastruktur deren Lese- und Schreibrechte eingeschränkt sind.
Polyzentrische Governance	Ein Governance-Ansatz, bei dem mehrere Parteien innerhalb eines Ökosystems Regeln und Strategien aushandeln, um gemeinsame Probleme zu lösen.
Proof-of-Stake	Ein Verfahren, mit dem ein Blockchain-Netzwerk einen Konsens erreichen kann, oft in dem energieintensive Berechnungen gelöst werden müssen.
Privacy by Default	Die Konzeption eines Systems mit solchen Voreinstellungen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt sind, soweit die betroffene Person nicht etwas anderes bestimmt.
Privacy by Design	Ein Ansatz, mit dem Schutz von Personendaten präventiv bei der technischen und organisatorischen Konzeption eines Systems gewährleistet wird.
Public-Key-Infrastructure	Eine Infrastruktur zur Ausstellung, Verteilung und Validierung von Schlüsselmaterialen, deren Zugehörigkeit zu bestimmten Organisationen bescheinigt wurde.
Schema	Eine Vorlage für einen digitalen Nachweis, welche dessen Inhalt spezifiziert (d. h. Metadaten inkl. Nutzungsbedingungen, Behauptungen, Beweismethode).
Self Sovereign Identity (SSI)	Ein Ansatz für das Identitätsmanagement, bei dem digitale Nachweise verwendet werden, um Attributinformationen über eine Person zu übermitteln (z. B. Name, Vorname, Geburtsdatum).
Software-Architekturrichtlinien	Vom technischen Betrieb festgelegte und durch die Geschäftsstelle genehmigte Richtlinien. Sie bestimmen, wie Software (z. B. Intelligente Verträge) für die Datenföderation zu entwickeln ist (z. B. Vorlagen für Standardabläufe oder Umsetzung der Sicherheitsvorkehrungen etc.).
Teilnehmende	Eine Partei der Datenföderation, die passiv mitwirken darf (z. B. Einsicht von öffentlichen Informationen im dezentralen Datenregister oder die Verifikation von Nachweisen). Solche Parteien müssen mit dem Betreiber oder mit der Betreiberin der Datenföderation in der Regel keinen Vertrag unterzeichnet haben.

Transaktion	Eine Transaktion ist eine Operation, mit der Daten in das dezentrale Datenregister übernommen werden können. Transaktionen beinhalten keine personenbezogenen Daten.
Überprüfer:in	Unter einer Überprüferin oder einem Überprüfer versteht man Personen oder Institutionen, welche die Validität von ihnen vorgelegten digitalen Nachweisen mithilfe der Informationen auf dem dezentralen Datenregister überprüfen.
(verifizierbarer) digitaler Nachweis	Im vorliegenden Kontext beinhaltet ein digitaler Nachweis eine oder mehrere Aussagen einer Institution oder Behörde (z. B. einer Schule oder eines Amtes) zu einem Subjekt (z. B. einer Lernenden). Ob diese Aussagen aus vertrauenswürdiger Quelle stammen, kann mithilfe der Daten auf dem dezentralen Datenregister überprüft werden – daher verifizierbarer digitaler Nachweis.
Zero Knowledge Proof	Ein Zero Knowledge Proof ist ein kryptografisches Protokoll. Es ermöglicht eine Aussage über Daten zu machen, ohne die eigentlichen Daten selbst preiszugeben (z. B. dass man über 18 Jahre alt ist, ohne das Geburtsdatum bekannt geben zu müssen).

educa

Erlachstrasse 21
3012 Bern

+41 31 300 55 00
info@educa.ch

Konzept der Datenföderation für die Berufsbildung
Teil 3 – Realisierungsplan und Kosten

1.3.2023

Digitaler Bildungsraum Schweiz
Espace numérique suisse de formation
Spazio formativo digitale svizzero
Spazi da furmazium digital svizzer
Swiss digital education space

educa

Inhalt

Management Summary

Im ersten Teil des Konzepts der Datenföderation für die Berufsbildung wurde der Fokus auf die künftige technische Infrastruktur gelegt. Damit wurden die Aspekte der Effizienzsteigerung, der Datenverfügbarkeit und der Anschlussfähigkeit betont. Der zweite Teil des Konzepts beinhaltete eine Sicht auf personenbezogene Daten wie auch eine adäquate Governance. Das Ziel des Data-Governance-Modells des zweiten Teils ist es, allen beteiligten Akteuren der Datenföderation eine kohärente, effektive Nutzung und einen sicheren und gesetzeskonformen Austausch von Daten zu ermöglichen.

Der nun vorliegende dritte Teil beschreibt den Zeitrahmen, die Kostenrechnung sowie die Reihenfolge der Umsetzung in Inkrementen etappieren für die Realisierung des Konzepts der Datenföderation. Zudem wird das Potential der Datenföderation anhand eines nächsten Anwendungsfalls detailliert ausgeleuchtet: der direkte und automatisierte Datenaustausch zwischen Berufsbildungsamt, üK-Anbietern und Lehrbetrieben. Der dritte Teil schliesst mit einer detaillierten Risikoanalyse für die Realisierungsphase.

Gelingensbedingung für die künftige Datenföderation ist die Schaffung regulierender Grundlagen. Einerseits benötigt die Organisation der Datenföderation eine gemeinsam von den Kantonen und gegebenenfalls des Bundes getragene Grundlage, damit die Datenföderation als solche in einem öffentlich-rechtlichen Kontext geschaffen werden kann. Andererseits kann sich ihr volles Potential erst dann entfalten, wenn – mit Blick auf die kantonalen Datenschutzregulierungen – sich die Datenweitergabe zwischen den Kantonen und innerhalb der Datenföderation auf eine stabile interkantonale Vereinbarung stützen kann.

Der Realisierungsplan geht von einer schrittweisen Umsetzung der Datenföderation aus. Die Realisierung beginnt notwendigerweise mit der Erarbeitung der Grundlagen. In diesem ersten Schritt sind insbesondere Elemente der Governance und Architektur zentral. Danach beginnt bereits der eigentliche Betrieb, in dem schrittweise in Inkrementen der Mehrwert der Datenföderation für die Nutzenden generiert wird. Die ersten vier geplanten Inkremente umfassen *die Ausstellung EFZ als digitaler Nachweis, die Anmeldung zum üK, Berufsschulzeugnisse als digitale Nachweise* und das *Erteilen der Bildungsbewilligung*. Für die Realisierung der Grundlagen und der ersten vier Inkremente wird mit einer Zeitdauer von höchstens drei Jahren gerechnet. Anschliessend können weitere Inkremente realisiert werden.

Das vorliegende Dokument beinhaltet den finalen von drei Teilen der Konzeption einer Datenföderation für die Berufsbildung. Die drei Konzeptteile zusammen bilden das Entscheiddossier zuhanden des Staatssekretariats für Bildung, Forschung und Innovation (SBFI) und der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK).

educa

1. Einführung

Im Zentrum dieses dritten Teils steht der Realisierungsplan zur Konzeptumsetzung (s. Kapitel 5). Er zeigt auf, wie das Konzept etappiert in Form von Inkrementen umgesetzt werden kann. Der Grundgedanke ist, dass die Abfolge der Inkremente für den Aufbau der Datenföderation in einem bestimmten Rahmen frei gewählt werden kann. Zwingend jedoch muss mit dem initialen Inkrement, den Grundlagen, begonnen werden.

Die einzelnen im Realisierungsplan beschriebenen Inkremente sind jeweils in vier Teilbereiche unterteilt: Governance, Architektur, Managementtätigkeiten und Begleitmassnahmen. Diese Teilbereiche werden jeweils in die wesentlichen Tätigkeiten mit der dazugehörigen Kostenschätzung aufgeschlüsselt (s. Kapitel 5). Den Regulierungsbedarf für die Schaffung der Datenföderation wird in Kapitel 4 analysiert.

Die Datenföderation fügt sich nahtlos in die Strategien des Bundes und der Kantone im Bereich E-Government ein. Mehrere Beispiele aus den Kantonen zeigen, dass ein dezentrales Datenregister oder eine Blockchain-Technologie eine geplante oder bereits angewandte Lösung im Bereich E-Government ist.

Öffentliche Hand	Projekt
Kanton Genf	Die Universität Genf stellt digitale Nachweise aus, die die Authentifizierung von Abschlüssen durch eine Blockchain erlauben. Das Amt für Inspektionen und Arbeitsverhältnisse nutzt für das Handelsregister Blockchain, um digitale Nachweise auszustellen.
Kanton Zürich	Die Zürich testet elektronische Brieftaschen und das Ausstellen von digitalen Nachweisen auf der Grundlage der Blockchain-Technologie.
Kanton Jura	Das Betreibungsregisteramt stellt digitale Belege aus, die dank der Blockchain-Technologie die Echtheit der Dokumente belegen.
Kanton Aargau	in einem Projekt wurde eine Blockchain eingesetzt, um Wohnsitzbescheinigungen in Form von digitalen Belegen auszustellen.
Kanton Schaffhausen	Das Betreibungsamt hat für den Betreibungsregisterauszug ein auf Blockchain basierendes Pilotprojekt und sein Projekt eID+ eingeführt.
Bund	Das Eidgenössische Personalamt prüft die Machbarkeit eines neuen digitalen Bundesmitarbeiterausweises im Zusammenhang mit der E-ID.

2. Die Prozesslandschaft der Datenföderation

Die Governance der Datenföderation (s. Kapitel 3 in Teil 2) sieht vor, dass bestimmte Strukturen und Praktiken vorhanden sein müssen, um sicherzustellen, dass die Datenföderation ihre Aufgaben erfüllt. Das Organisationsmodell bestimmt weitgehend die Strukturen und die Art der Verantwortlichkeiten und der Rechenschaftspflicht zwischen ihnen (s. Kapitel 3.1 in Teil 2). Diese Struktur wiederum bedarf einer Prozesslandschaft – also einen Überblick über alle bestehenden Prozesse und Aufgaben, die durch die Geschäftsstelle zu bewerkstelligen

sind. Abbildung 1 fasst diese Prozesslandschaft zusammen. Die in Abbildung 1 gezeigte Struktur ist teilweise an das COBIT-Rahmenmodell (engl. «control objectives for information and related technology») angelehnt, wurde aber an die Gegebenheiten der Berufsbildung in der Schweiz angepasst. Die folgende Tabelle gibt einen Überblick über die wichtigsten Prozessgruppen dieser Struktur:

Tabelle 1: Prozessgruppen der Datenföderation

Prozessgruppe	Zuständigkeit	Beschreibung
Governance und Steuerung	Bildungspolitische Gremien	Die gesamte politische Trägerschaft und Koordination zwischen Bund, Kantonen und Akteuren der Berufsbildung sowie die Aufsicht über die Finanzierung der Datenföderation.
Planung, Ausrichtung und Organisation	Geschäftsstelle	Alle Führungsaufgaben, die zur Sicherstellung des Erfolgs der Datenföderation erforderlich sind inkl. Ressourcenplanung, Qualitätsmanagement und Rechenschaftspflicht.
Beschaffung und Weiterentwicklung	Geschäftsstelle	Alle Aktivitäten im Zusammenhang mit der kontinuierlichen Weiterentwicklung der Datenföderation, von der Sicherstellung einer angemessenen Data Governance und Regulierung bis hin zur Konzeption und Entwicklung neuer Funktionalitäten.
Service Delivery und Support	Geschäftsstelle (Lifecycle Management) Technischer Betrieb (IT Betrieb, Betriebskontinuität)	Alle Aktivitäten rund um den Lebenszyklus der Mitgliedschaft (d. h. Beitritt, Support, Austritt) sowie den technischen Betrieb und Wartung der Infrastruktur und die Kontinuität der darauf laufenden Dienste.
Leistungsmessung und -sicherung	Geschäftsstelle in Zusammenarbeit mit externen Audit-Stellen	Alle Aufgaben rund um die Bewertung der Datenföderation, die Erfüllung der rechtlichen Anforderungen , umgemäss den geltenden Normen und Praktiken zu funktionieren.

Damit diese Prozesslandschaft der Geschäftsstelle mit der schrittweisen Einführung der Datenföderation mitwächst (s. Kapitel 5.1), muss sie nach der Erarbeitung der Grundlage und vor der Implementierung jedes Inkrements noch einmal überarbeitet beziehungsweise erweitert werden. Darüber hinaus gibt es in der Prozesslandschaft Schnittstellen zwischen den Prozessen. Diese Feedbackschleifen sind in Abbildung 1 als Pfeile ersichtlich.

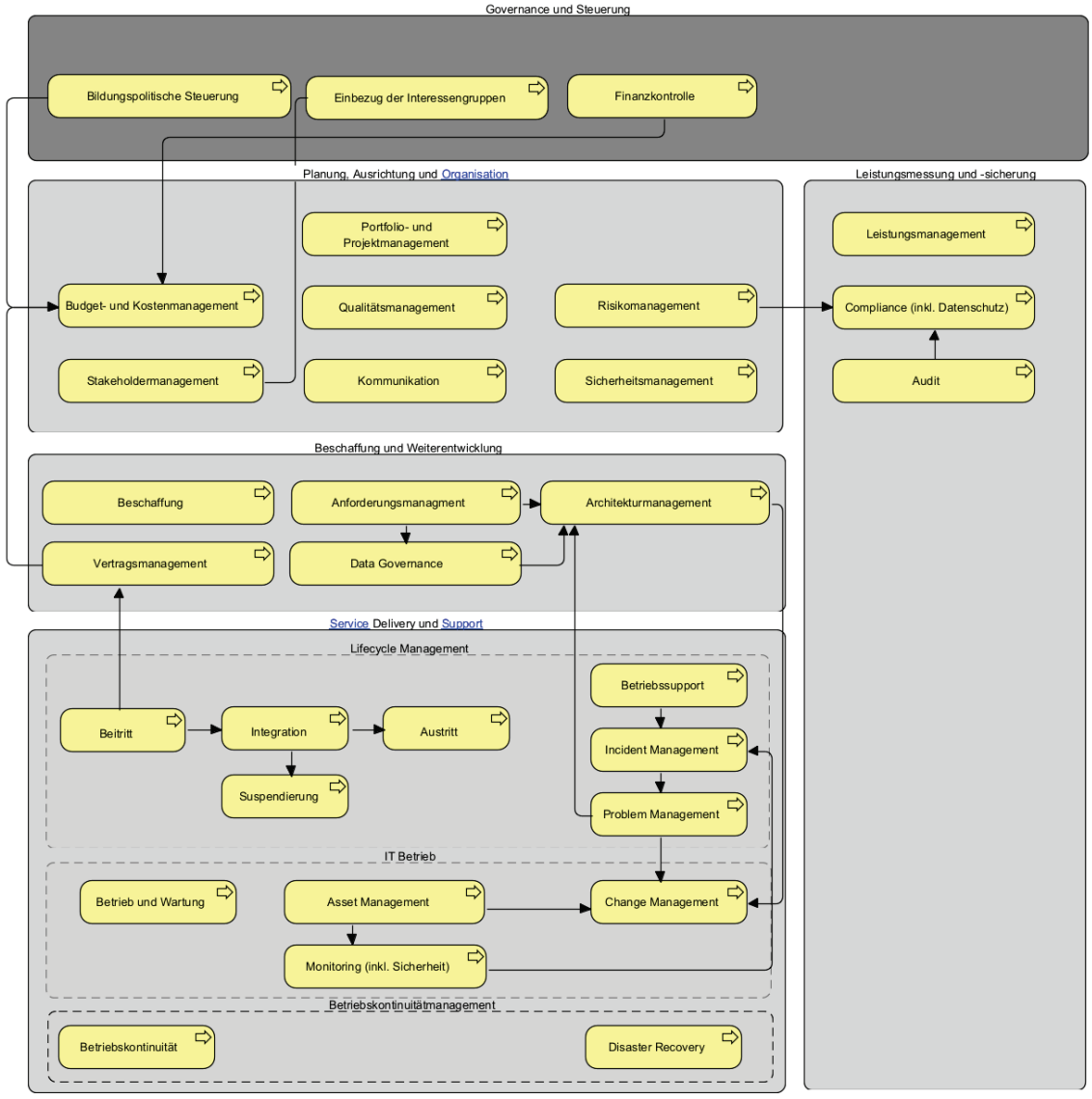

Abbildung 1 : Prozesslandschaft für die Geschäftsstelle der Datenföderation

3. Anwendungsfall: Der direkte Datenaustausch zwischen Berufsbildungsamt, üK-Anbietern und Lehrbetrieben

In der vorgeschlagenen Datenföderation interagieren verschiedene Individuen und Institutionen miteinander. Dies geschieht unter anderem durch den Austausch von digitalen Nachweisen – also Nachweisen, die eine oder mehrere Aussagen zumeist einer Institution oder Behörde (z. B. einer Berufsfachschule) zu einem Subjekt (z. B. einer Lernenden) enthalten. Das folgende Kapitel und der dazugehörige Anwendungsfall zeigen einerseits, wie Unternehmen und Institutionen die Datenföderation über elektronische Brieftaschen nutzen (im Unterschied zum Anwendungsfall in Kapitel 3.1 im Teil 1, bei dem die Lernenden im Zentrum

stehen). Zum anderen konkretisiert der Anwendungsfall, wo die in Kapitel 3.3 in Teil 1 beschriebenen Architekturprinzipien in der praktischen Umsetzung der Datenföderation zum Tragen kommen. Schliesslich verdeutlicht dieses Kapitel und der dazugehörige Anwendungsfall, wie die Datenföderation heutige Datenaustauschprozesse beschleunigt und automatisiert.

Die Anforderungen an die hier im Vordergrund stehenden organisationsinternen elektronischen Brieftaschen unterscheiden sich deutlich von den Anforderungen an eine private elektronische Brieftasche (s. Kapitel 3.1 in Teil 1). Konkret: Die organisationsinterne elektronische Brieftasche gehört dem Unternehmen oder der Institution. Allerdings müssen deren Mitarbeitende mit dieser elektronischen Brieftasche interagieren um digitale Nachweise auszustellen, zu erhalten und zu verifizieren. Diese Interaktion findet über eine spezifische Applikation, die dem Erscheinungsbild nach mit einer heutigen Applikation vergleichbar ist, oder über eine herkömmliche Schulverwaltungslösung statt. Neu ist jedoch die Art und Weise, wie Datenaustauschprozesse im Hintergrund geschehen.

Damit Mitarbeitende mit der organisationsinternen elektronischen Brieftasche arbeiten können, sind organisationsinterne Regelungen notwendig. Dazu gehören zum Beispiel die Zugriffsrechte von Mitarbeitenden auf bestehende unternehmensspezifische Nachweise (wie die Bildungsbewilligung), die Verteilmechanismen für eingehende Nachweise an die zuständigen Mitarbeitenden oder die Berechtigung für Mitarbeitende, das Unternehmen in einer direkten Verbindung mit einem anderen Mitglied oder Teilnehmenden der Datenföderation zu vertreten (folgt aus Architekturprinzipien AP.G.5: «Legitimierter Zugang zur Datenföderation»; AP.S.1: «Rollenbasierte Zugangskontrolle» und AP.S.2: «Identitätssicherung der Komponenten»). Denkbar ist, dass sich Mitarbeitende durch das Vorzeigen eines entsprechenden digitalen Nachweises, bei ihrer organisationsinternen elektronischen Brieftasche anmelden (dieser Anmeldungsprozess ist im untenstehenden Anwendungsfall der Einfachheit halber nicht aufgeführt). Die Gültigkeit dieser digitalen Nachweise wird dann von der organisationsinternen elektronischen Brieftasche über eine Abfrage einer firmeneigenen Datenbank geprüft. Dadurch weiss die organisationsinterne elektronische Brieftasche auch, welche Zugriffs- und Bearbeitungsrechte eine Person hat. Dadurch können Abläufe, wie die Zuweisung von Anfragen an bestimmte Personen, automatisiert.

Alle Institutionen und Unternehmen müssen diese Zugriffsrechte, Verteilmechanismen und weitere Regelungen zur organisationsinternen elektronischen Brieftasche selbständig in einem Governance-Modell definieren und in der technischen Architektur ihrer organisationsinternen elektronischen Brieftasche umsetzen. Die einzige Anforderung, welche durch die Datenföderation an solche organisationsinternen Regelwerke gestellt wird, ist die Anschlussfähigkeit der organisationsinternen elektronischen Brieftasche an die Datenföderation.

Ist die Anschlussfähigkeit garantiert, bieten organisationsinterne elektronische Brieftaschen für Institutionen und Unternehmen das Potenzial, den Datenaustausch in der Berufsbildung zu vereinfachen und zu automatisieren. Zwei konkrete Beispiele verdeutlichen dies im nachstehend Anwendungsfall: 1) Die Genehmigung des Lehrvertrags von Alina, einer Auszubildenden Malerin EFZ, durch das Berufsbildungsamt und 2) die Anmeldung von Alina und ihren Berufslehrkolleginnen und -kollegen zu den überbetrieblichen Kursen (üK).

Direkter Datenaustausch mithilfe organisationsinterner elektronischer Brieftaschen

Die untenstehende Tabelle 2 sowie Abbildung 2 beschreiben, wie Alinas Berufsbildnerin und ein Mitarbeiter des Berufsbildungsamtes über ihre jeweiligen organisationsinternen elektronischen Brieftaschen die Genehmigung von Alinas Lehrvertrag abwickeln. Die Einreichung von Alinas ausgefülltem Lehrvertragsformular geschieht – wie im entsprechenden HAKA-Prozess vorgesehen – durch den Lehrbetrieb, in unserem Fall durch Alinas künftige Berufsbildnerin. Dabei wird das Lehrvertragsformular wie bisher vervollständigt und eingereicht. Der weitere Datenaustausch zwischen Berufsbildungsamt, Lehrbetrieb, üK-Anbieter und Alina findet über die Datenföderation statt. Welche Architekturprinzipen der Datenföderation dabei in jedem Schritt des Datenaustauschprozesses zum Tragen kommen, wird aus der letzten Spalte in Tabelle 2 ersichtlich.

Tabelle 2: Datenaustausch und entsprechende Architekturprinzipien zur Genehmigung eines Lehrvertrages

Schritte im Datenaustauschprozess	Architekturprinzipien, die zum Tragen kommen (s. Kapitel 3.3 in Teil 1 des Konzepts)
1. Bevor der Lehrvertrag genehmigt werden kann, muss das Berufsbildungsamt prüfen, ob der Lehrbetrieb über die entsprechende Bildungsbewilligung verfügt. Der Mitarbeiter des Berufsbildungsamtes stellt daher bei Eingang des Lehrvertragsformulars über die organisationsinterne elektronische Brieftasche des Amtes und über eine bereits bestehende, sichere und direkte Verbindung (Alina ist nicht der erste Lernende dieses Betriebs) eine Anfrage an den Lehrbetrieb. In dieser Anfrage bittet der Mitarbeiter den Lehrbetrieb darum, ihm die bereits als digitaler Nachweis ausgestellte Bildungsbewilligung als digitales Dossier vorzulegen (dies im Unterschied zum heutigen Prozess).	• AP.G.1: Föderalistische Datenhaltung • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.D.1: Daten sind ein gemeinsames Gut im Dienst der Berufsbildung • AP.N.1: Direkter Datenaustausch
2. Die organisationsinterne elektronische Brieftasche des Lehrbetriebs ist so konfiguriert, dass sie auf diese Anfrage automatisch und in Echtzeit reagiert und dem Berufsbildungsamt ein digitales Dossier zur Bildungsbewilligung übermittelt. Es braucht also keinen manuellen Eingriff von Alinas Berufsbildnerin.	• AP.G.1: Föderalistische Datenhaltung • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.D.1: Daten sind ein gemeinsames Gut im Dienst der Berufsbildung • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation

3.	Auch die Prüfung der Gültigkeit der Bildungsbewilligung geschieht automatisch. Nachdem das digitale Dossiers zur Bildungsbewilligung in der organisationsinternen elektronischen Brieftasche des Berufsbildungsamtes eintrifft, führt diese Brieftasche eine automatisierte Abfrage auf dem dezentralen Datenregister durch. Der Mitarbeitende des Berufsbildungsamtes muss also nur noch prüfen, ob für die Gültigkeit des Lehrvertrags alle Informationen vorhanden sind - alles andere geschieht im Hintergrund.	• AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.G.4: Transparenz, Integrität und Verantwortlichkeit über bildungsrelevante Ereignisse • AP.N.1: Direkter Datenaustausch • AP.N.3: Asynchronität der Kommunikation
4.	Nach erfolgter Prüfung erstellt der Mitarbeitende des Berufsbildungsamtes in der Applikation, welche auf die organisationsinterne elektronische Brieftasche zugreift, einen digitalen Nachweis des Lehrvertrages. Dazu verwendet der Mitarbeitende ein auf dem öffentlich zugänglichen Datenregister abgelegtes Schema.	• AP.D.3: Semantische Interpretierbarkeit der Daten • AP.N.1: Direkter Datenaustausch • AP.N.3: Asynchronität der Kommunikation
5.	Danach sendet der Mitarbeiter des Berufsbildungsamtes den digitalen Nachweis des Lehrvertrags über die Datenföderation an Alinas Lehrbetrieb, mit dem Hinweis, dass der Lehrvertrag genehmigt ist. Der Lehrbetrieb kann sich jetzt offiziell als «Alinas Lehrbetrieb» ausweisen. Alinas Berufsbildnerin wird durch die organisationsinterne elektronische Brieftasche über den Eingang des digitalen Nachweises informiert.	• AP.G.1: Föderalistische Datenhaltung • AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen
6.	Durch die Genehmigung des Lehrvertrages wird in der organisationsinternen elektronischen Brieftasche des Berufsbildungsamt automatisch eine Verbindungseinladung für Alina generiert und zum Beispiel in Form eines QR-Codes an Alina verschickt (für Details zum Verbindungsaufbau, vgl. Anwendungsfall «Lucas digitale Nachweise» in Teil 1 des Konzepts zur Datenföderation).	• AP.S.3: Identitätssicherung der betroffenen Parteien • AP.N.1: Direkter Datenaustausch • AP.N.3: Asynchronität der Kommunikation
7.	Alina scannt die Anfrage und nimmt sie über die private elektronische Brieftasche auf ihrem mobilen Endgerät an (für Details zur allfälligen Prüfung von Alinas Identität, vgl. Anwendungsfall «Lucas digitale Nachweise» in Teil 1 des Konzepts zur Datenföderation).	• AP.S.3: Identitätssicherung der betroffenen Parteien • AP.N.1: Direkter Datenaustausch

8.	Durch die Annahme der Verbindungseinladung wird der genehmigte Lehrvertrag – wiederum automatisiert – durch die organisationsinterne elektronische Brieftasche, als digitaler Nachweis über die sichere Verbindung an Alina versandt.	• AP.G.1: Föderalistische Datenhaltung • AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation
9.	Mit dem Erstellen des digitalen Nachweises für den Lehrvertrag erhält zeitgleich auch der zuständige üK-Anbieter über eine bereits bestehende direkte und sichere Verbindung eine Meldung (vgl. Begrifflichkeiten im Anhang) über Alinas Lehrvertragsgenehmigung. Diese Meldung dient als Voranmeldung zum überbetrieblichen Kurs (üK) und enthält nur minimale Daten wie den Beruf, die Fachrichtung und den Lehrbetrieb. Sofern Alinas künftiger üK-Leiter der organisationsinternen elektronischen Brieftasche die Berechtigung erteilt hat, wird diese Meldung auch direkt an ihn weitergeleitet. Somit wissen der üK-Anbieter sowie Alinas künftiger üK-Leiter frühzeitig, wie viele Kurse angeboten werden müssen. Dies hilft bei der Planung des üK-Angebots und dessen Umsetzung.	• AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation

Die Tabelle 3 beschreibt den Datenaustausch und die betroffenen Architekturprinzipien des zweiten Beispiels – der Anmeldung von Alina zum üK durch den üK-Anbieter. Für die definitive Anmeldung zum üK schickt der üK-Anbieter eine Anfrage an die gemeldeten Lernenden, also auch an Alina. Dazu sind die folgenden Schritte notwendig, welche auch in Abbildung 2 aufgeführt sind:

Tabelle 3: Datenaustausch und betroffene Architekturprinzipien zur definitiven Anmeldung an einen üK

Schritte im Datenaustauschprozess	Architekturprinzipien, die zum Tragen kommen (s. Kapitel 3.3 in Teil 1 des Konzepts)
1. Alinas künftiger üK-Leiter erstellt mithilfe der organisationsinternen elektronischen Brieftasche des üK-Anbieters eine Einladung für eine sichere und direkte Verbindung mit Alina und sendet diese an Alina, zum Beispiel als QR-Code in einem E-Mail (für Details zur allfälligen Prüfung von Alinas Identität, vgl. Anwendungsfall «Lucas digitale Nachweise» in Teil 1 des Konzepts zur Datenföderation).	• AP.S.3: Identitätssicherung der betroffenen Parteien • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen
2. Alina scannt diesen QR-Code mit ihrer persönlichen elektronischen Brieftasche und nimmt die Verbindung an. Dieser Kommunikationskanal bleibt während der gesamten Ausbildungsdauer bestehen, da über diese Verbindung später auch üK-Kompetenznachweise als digitale Nachweise übermittelt werden können.	• AP.S.3: Identitätssicherung der betroffenen Parteien • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation
3. Daraufhin versendet die organisationsinterne elektronische Brieftasche des üK-Anbieters eine automatische Anfrage an Alina, mit der Bitte, sie solle alle für den üK noch notwendigen Detailinformationen als digitales Dossier übermitteln. Die Anfrage enthält dabei klare Angaben darüber, welche Daten von Alina benötigt werden.	• AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.D.1: Daten sind ein gemeinsames Gut im Dienst der Berufsbildung • AP.D.3: Semantische Interpretierbarkeit der Daten • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation

4.	Alina erhält daraufhin eine Anfrage in ihrer persönlichen elektronischen Brieftasche. Sie gibt die gewünschten Informationen frei. So wird das digitale Dossier über die direkte verschlüsselte Verbindung an die organisationsinterne elektronische Brieftasche des üK-Anbieters zurückgeschickt. Das Dossier umfasst unter anderem Daten zu Alinas Person, aber auch zu ihrem Bildungsverhältnis (z. B. auch Kontaktdaten ihrer Berufsbildnerin).	• AP.G.1: Föderalistische Datenhaltung • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.D.1: Daten sind ein gemeinsames Gut im Dienst der Berufsbildung • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation
5.	Bei der organisationsinternen elektronischen Brieftasche des üK-Anbieters angekommen, wird das Dossier mithilfe einer Abfrage des dezentralen Datenregisters automatisch auf Gültigkeit geprüft. Das Dossier basiert auf einem gültigen digitalen Nachweis. Alinas künftiger üK-Leiter wird über den Eingang des Dossiers informiert und Alina ist somit zum üK angemeldet.	• AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.G.4: Transparenz, Integrität und Verantwortlichkeit über bildungsrelevante Ereignisse • AP.N.1: Direkter Datenaustausch • AP.N.3: Asynchronität der Kommunikation
6.	Durch die Anmeldung wird von der organisationsinternen elektronischen Brieftasche automatisch und umgehend eine Anfrage für den Aufbau einer direkten und verschlüsselten Verbindung an Alinas Berufsbildnerin versandt, zum Beispiel als Link in einer E-Mail.	• AP.S.3: Identitätssicherung der betroffenen Parteien • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation
7.	Alinas Berufsbildnerin öffnet diesen Link über ihre Applikation, welche auf die organisationsinterne elektronische Brieftasche zugreift, und nimmt die Verbindung an.	• AP.S.3: Identitätssicherung der betroffenen Parteien • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.3: Asynchronität der Kommunikation

8.	Sogleich geht in der organisationsinternen elektronischen Brieftasche von Alinas Lehrbetrieb die Meldung ein, dass Alina zum üK angemeldet ist. Alinas Berufsbildnerin wird von der organisationsinternen elektronischen Brieftasche automatisch über den Eingang dieser Meldung informiert, da sie der Übermittlung solcher Benachrichtigungen zugestimmt hat.	• AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation
9.	Sobald die ersten üK-Termine feststehen, kann der üK-Leiter (oder die Administration des üK-Anbieters) Alina über die direkte Verbindung dazu aufbieten.	• AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation
10.	Auch Alinas Lehrbetrieb, und über dessen organisationsinterne elektronische Brieftasche Alinas Berufsbildnerin, erhalten eine Meldung über das üK Aufgebot.	• AP.G.3: Verfügbarkeit von Daten bei Entscheidungsfindungen • AP.S.5: Sicherer und rechtskonformer Datenaustausch • AP.N.1: Direkter Datenaustausch • AP.N.2: Atomarität von Bildungsereignissen • AP.N.3: Asynchronität der Kommunikation

Dank der Datenföderation hat Alinas üK-Leiter immer einen aktuellen Überblick über die Anzahl Teilnehmenden an seinem üK. Sollte Alina zudem, zum Beispiel aus Krankheitsgründen, einmal nicht an einem üK teilnehmen, kann sie ihre Abwesenheit über die bestehende direkte Verbindung dem üK-Anbieter melden (und wenn nötig mit einem Arztzeugnis in Form eines digitalen Dossiers ergänzen). Alinas üK-Leiter wird so umgehend informiert und kann die Abwesenheit erfassen. Dadurch wird wiederum eine Meldung an Alinas Lehrbetrieb (und damit ihre Berufsbildnerin) ausgelöst, dass Alina den üK wegen Krankheit verpasst hat. So trägt die Datenföderation dazu bei, dass alle notwendigen Informationen in Echtzeit und über direkte verschlüsselte Verbindungen den jeweiligen Akteuren bekannt sind.

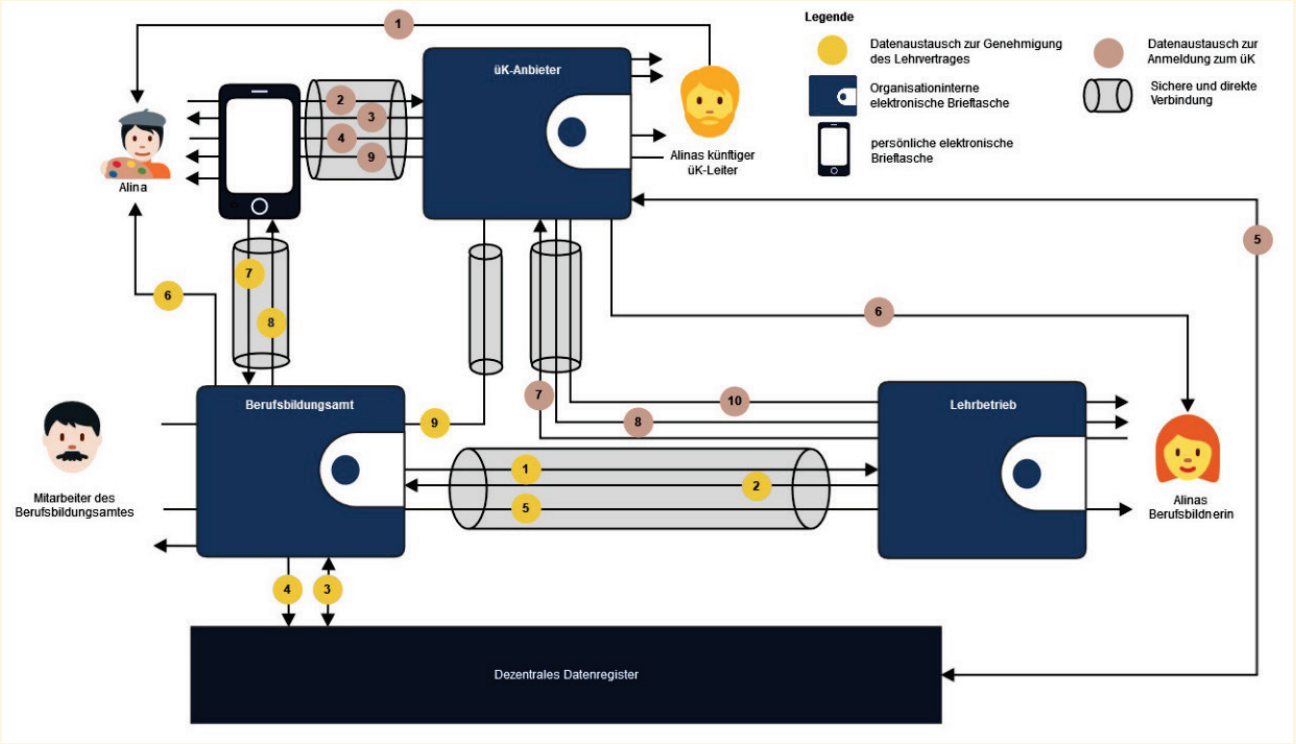

Abbildung 2: Die Genehmigung von Alinas Lehrvertrag und ihre Anmeldung zum üK

4. Regulierungsbedarf für die Datenföderation: Interkantonale Vereinbarungen

Eine künftige Datenföderation wird gemäss vorliegendem Konzept in einem öffentlich-rechtlichen Kontext geschaffen und betrieben werden. Die Schaffung der Organisation «Datenföderation» bedarf einer Vereinbarung zwischen den Trägern. Einmal in Betrieb wird die Datenföderation zu einer Vereinfachung der Datenweitergabe durch Kantone in einem gesamtschweizerischen Rahmen führen. Diese Datenweitergabe und die damit verbundene Bearbeitung personenbezogener Daten wird unter Berücksichtigung der kantonalen Datenschutzgesetzgebungen stattfinden müssen. Eine Analyse zeigt, dass sich das Potenzial der Datenföderation auf Basis einer gemeinsamen Interkantonalen Vereinbarung über die Datenweitergabe besser entfalten könnte.

4.1 Schaffung der Datenföderation

Gemäss den Zuständigkeiten hat der Bund das Bundesgesetz über die Berufsbildung (BBG) erlassen. Dieses Gesetz wird durch Verordnungen ergänzt. Die ordnungsgemässe Ausführung liegt bei den Kantonen. Zu beachten gilt, dass der Bund die Kantone nicht zwingen kann einer interkantonalen Vereinbarung über die Berufsbildung beizutreten (im Gegensatz zum Bereich der öffentlichen Bildung). Der Bund ist auch im Bereich E-Government nicht befugt, den Kantonen organisatorische Massnahmen vorzuschreiben. Daran erinnerte die Bundeskanzlei, als sie 2011 zur Frage der Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen Bund und Kantonen Stellung nahm. Diese Stellungnahme führte dazu, dass der Bund und die Kantone eine Rahmenvereinbarung über E-Government unterzeichneten, um die Zusammenarbeit zwischen dem Bund und den Kantonen in diesem Bereich zu fördern. Seit 2022 ist auf Basis der «Öffentlich-rechtlichen Rahmenvereinbarung über die Digitale Verwaltung Schweiz» von Bund und Kantonen die Digitale Verwaltung Schweiz (DVS) aktiv.

Die Datenföderation verfolgt insbesondere das Ziel den Datenaustausch zwischen den Verbundpartnern im Bereich der Berufsbildung zu vereinfachen. Damit die Institutionen der Mitgliedskantone die Datenföderation auf kollaborative, einheitliche und interoperable Weise nutzen können, bedarf es gemeinsamer organisatorischer Regelungen. Die Entscheidung, die gemeinsame Datenföderation zu schaffen und ihr beizutreten, liegt unserer Ansicht nach im Bereich des E-Government und obliegt somit den Kantonen. Aus den oben genannten Gründen erscheint uns eine interkantonale Vereinbarung notwendig. Diese ermöglicht die Gründung der Datenföderation und damit den Kantonen, sich gegenseitig zu unterstützen und ihre organisatorischen Anstrengungen im Bereich der Berufsbildung zu bündeln. Der Begriff Vereinbarung ist in diesem Text im allgemeinen Sinne zu verstehen, ohne zwischen den Begriffen Konkordat, Abkommen, Reglement oder Vertrag zu unterscheiden. Weitere Parameter wie die Form der Datenföderation, das anwendbare Recht sowie die Finanzierung müssen geregelt werden. Da die Berufsbildung eine Bundeskompetenz ist, ist der Bund ein wichtiger Partner für die Kantone.

Die Erarbeitung dieses Elements ist im Rahmen der Entwicklung der Grundlagen (s. Kapitel 5.1) eingeplant.

4.2 Interkantonaler Datenaustausch

Damit Daten zwischen den Mitgliedern der Datenföderation aus verschiedenen Kantonen ausgetauscht werden können, empfiehlt sich die Harmonisierung der kantonalen Datenschutzbestimmungen. Dies bietet sich an, da die kantonalen Institutionen ihren eigenen Rahmengesetzen zum Datenschutz unterliegen. Zudem wird das BBG durch die Kantone angewandt. Es enthält jedoch keine Präzisierungen zum interkantonalen Datenaustausch. Durch eine Harmonisierung der kantonalen Datenschutzbestimmungen kann das volle Potenzial der Datenföderation ausgeschöpft werden.

Das Fehlen einer solchen Vereinbarung stellt jedoch kein Hindernis für die Umsetzung der Datenföderation dar, solange die Daten zwischen den Einrichtungen desselben Kantons im Einklang mit den geltenden Gesetzen weitergegeben werden können. Kantone, die für die Datenweitergaben an andere Kantone bereits erste Vereinbarungen basierend auf ihren jeweiligen kantonalen gesetzlichen Grundlagen getroffen haben, können ebenfalls von einer künftigen interkantonalen Vereinbarung im Zusammenspiel mit der Datenföderation profitieren.

Die Erarbeitung dieses Elements ist nicht Teil des Realisierungsplans.

5. Realisierungsplan der Datenföderation

Der Realisierungsplan sieht einen modularen Ansatz vor, bei dem neue Funktionen in Inkrementen zusammengefasst werden, die auf gemeinsamen Grundlagen beruhen. Durch den modularen Ansatz können die zu erbringenden Leistungen relativ unabhängig voneinander entwickelt und erbracht werden, wodurch sich Möglichkeiten zur flexiblen Gestaltung der Realisierung ergeben. Diese funktionale Strukturierung der Datenföderation steht im Einklang mit dem Betriebsmodell (z. B. Prozesslandschaft) und ermöglicht somit eine reibungslose Erweiterung der Dienste, ohne dass es zu Störungen im Tagesgeschäft kommt.

Die Umsetzung der Datenföderation erfolgt inkrementell. Jedes Inkrement wird in enger Zusammenarbeit mit den Beteiligten schrittweise umgesetzt. Dies ermöglicht kontinuierliches Lernen und generiert einen direkten Mehrwert für die Berufsbildung. Folgende Elemente sind im Realisierungsplan vorgesehen:

- Grundlagen: Die Schaffung von Governance- und architektonischen Grundlagen, die für die Einrichtung einer Erstinfrastruktur für nachfolgende Inkremente erforderlich sind (inkl. die Ausschreibung des technischen Betriebs).
- Inkrement #1: Ausstellung EFZ als digitaler Nachweis
- Inkrement #2: Anmeldung zum üK
- Inkrement #3: Berufsschulzeugnisse als digitale Nachweise
- Inkrement #4: Erteilen der Bildungsbewilligung
- Weitere Inkremente je nach Bedarf (diese sind im Realisierungsplan nicht inbegriffen)

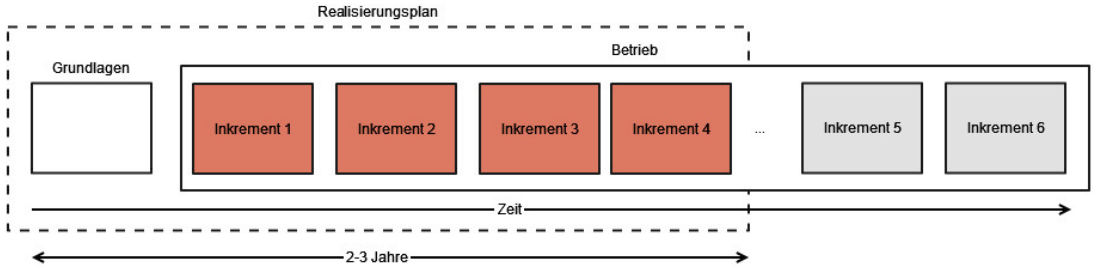

Abbildung 3:Schematischer Ablauf der Realisierung

Jedes Inkrement beinhaltet folgende Kategorien:

- Governance: Alle Angelegenheiten, die sich mit der Aufsicht und Regulierung der Datenföderation beschäftigen, einschliesslich der bildungspolitischen Steuerung sowie formeller Systeme für Audit und Compliance (z. B. ISMS) und sonstige Vereinbarungen (z. B. Standards, Organisationsreglement, Verträge).
- Architektur: Alle technischen und organisatorischen Massnahmen, die den ordnungsgemässen Betrieb der Datenföderation gemäss den Architekturprinzipien gewährleisten. Dies umfasst nicht nur die technische Infrastruktur und Komponenten (inkl. sonstige Schnittstelle innerhalb der Berufsbildung), sondern auch die Prozesse der Geschäftsstelle.
- Betrieb: Alle Aktivitäten rund um den täglichen Betrieb der Datenföderation (z. B. Wartung der Infrastruktur, Tätigkeiten der Geschäftsstelle etc.).
- Management: Unterstützende Tätigkeiten im Zusammenhang mit der Organisation, Ressourcenplanung und Kontrolle der Arbeit (z. B. Projekt- und Risikomanagement, Kostenkontrolle und Personalmanagement).
- Begleitmassnahmen: Unterstützende Aktivitäten, die sicherstellen, dass die Ergebnisse erfolgreich genutzt werden können (z. B. Dokumentation, Schulung und Kommunikation).

5.1 Detaillierung des Realisierungsplans

Im Folgenden werden die primären Projektaufgaben für die Realisierung der Datenföderation dargestellt. Ausgenommen von dieser Auflistung sind alle operativen Aufgaben, die die Geschäftsstelle und den Betrieb der Infrastruktur betreffen. Der geschätzte Aufwand wird in Form von Personentagen berechnet, denen später im Kostenmodell unterschiedliche Sätze zugeordnet werden. Darüber hinaus entstehen in einigen Fällen zusätzliche Drittkosten (z. B. Dienstleistungen, Lizenzen etc.), die ebenfalls im Kostenmodell berücksichtigt sind:

Realisierungsplan	Aufwand (Personal)		Dritt-kosten
Grundlagen	**PT/int**	**PT/ext**	**fällig**
Governance			
Bildungspolitische Steuerung	24	0	
Leistungsvereinbarung, Organisationsreglement und Organisationsmodell	20	10	
Einbindung der Anspruchsgruppen	20	0	
Prozesslandschaft Geschäftsstelle und Betriebskonzept	54	0	
Grundlagen des Vertragsmanagements (d. h. SLA, Föderationsverträge)	20	5	
Data Governance Framework und Standards	20	0	
Informationssicherheitsmanagementsystem (ISMS, ISO:IEC 27001:2022) und Datenschutzfolgenabschätzung (DSFA)	10	10	
Rechtsberatung und -belehrung	0	20	
Zusatzaufwand im Zusammenhang mit delegierten Aufgaben (z. B. Koordination)	5	25	
Architektur			
Basisinfrastruktur (Knoten, dezentrales Datenregister und Netzwerk)	35	30	
Identitäts- und Sicherheitsinfrastruktur (inkl. Edulog, E-ID) inkl. Datenschutz	10	20	
Qualitätsmanagement, Testing und Validierung	25	15	
Technische Supportinfrastruktur (z. B. Container Repo, Versionierung etc.)	5	1	X
Management			
Ausschreibung des technischen Betriebs	10	5	
Projektmanagement (inkl. Risikomanagement)	24	0	
Administration und Support (z. B. HR, Buchhaltung etc.)	10	0	
Betrieb			
Betrieb der Basis-IT-Infrastruktur (Grundinfrastruktur und Netzwerkdienste)	0	60	X
Managed Servers und Containers	0	0	X
Storage und Backups	0	0	X
Betrieb der Geschäftsstelle	24	0	
Begleitmassnahmen			
Dokumentation der technischen Richtlinien	24	0	
Webauftritt inkl. Markenschutz der Datenföderation	20	20	X
Kommunikation mit den Anspruchsgruppen (inkl. Webauftritt, Informationsanlässe etc.)	2	0	X

Realisierungsplan	Aufwand (Personal)		Dritt-kosten
Inkrement #1: Ausstellung EFZ als digitaler Nachweis	**PT/int**	**PT/ext**	**fällig**
Governance			
Datenarchitektur des dezentralen Datenregisters zum Zweck der Ausstellung von EFZ	5	5	
Informationssicherheits- und Datenschutzkonzept (ISDS) für das Inkrement 1	5	5	
Beratung bei den Prozessen der Berufsbildung	20	0	
Architektur			
Basisentwicklung der Infrastruktur für die Ausstellung von EFZ	15	30	
Konfiguration der Infrastruktur zum Anschluss von Standard Wallet-Applikationen	5	10	
Prozeduren zur Erstellung und Prüfung von digitalen EFZ	10	20	
Onboarding der bestehenden Applikationen	0	0	
Entwicklung, Konfiguration inkl. Zugriffsrechte der Agenteninfrastruktur	10	5	
Integration in die administrativen Abläufe der Geschäftsstelle	10	0	
Technische und organisatorische Massnahmen im Bereich Informationssicherheit und Datenschutz	20	5	X
Qualitätsmanagement, Testing und Validierung	10	15	
Management			
Projektmanagement (inkl. Risikomanagement)	24	0	
Administration und Support (z. B. HR, Buchhaltung etc.)	10	0	
Betrieb			
Laufende technische Betriebskosten (pro rata)	0	60	X
Betrieb der Geschäftsstelle	34	0	
Begleitmassnahmen			
Technische Spezifikation der Agenten	10	5	
Unterstützung der Berufsbildungsämter bei der Anpassung der Ausstellungsprozesse	24	0	
Kommunikationsmassnahmen zuhanden der Anspruchsgruppen im Kontext «digitales EFZ»	20	0	
Sensibilisierungsmassnahmen für SuS/Jugendliche	20	0	

Realisierungsplan	Aufwand (Personal)		Drittkosten
Inkrement #2: Anmeldung zum üK	**PT/int**	**PT/ext**	**fällig**
Governance			
Datenarchitektur des dezentralen Datenregisters zum Zweck der Anmeldung am üK	5	2	
Informationssicherheits- und Datenschutzkonzept (ISDS) für das Inkrement 2	5	2	
Beratung bei den Prozessen der Berufsbildung	20	0	
Architektur			
Technische Infrastruktur und Prozeduren zum Anmelden von Lernenden an üKs	15	20	
Spezifikation und Konfiguration der Cloud-Agenten-Infrastruktur	10	0	
Entwicklung einer Standard Controller-Applikation für Lehrbetriebe und Organisationen der Arbeitswelt (OdA)	10	50	
Entwicklung, Konfiguration inkl. Zugriffsrechte der Agenteninfrastruktur	15	5	
Integration in die administrativen Abläufe der Geschäftsstelle	10	0	
Technische und organisatorische Massnahmen im Bereich Informationssicherheit und Datenschutz	15	5	
Qualitätsmanagement, Testing und Validierung	10	15	
Management			
Projektmanagement (inkl. Risikomanagement)	15	0	
Administration und Support (z. B. HR, Buchhaltung etc.)	10	0	
Betrieb			
Laufende technische Betriebskosten (pro rata)	0	60	X
Betrieb der Geschäftsstelle	34	0	
Begleitmassnahmen			
Technische Spezifikation für die Controller und deren Agenten	10	5	
Unterstützung der OdA und Lehrbetriebe bei der Anpassung der Anmeldeprozesse	30	0	
Kommunikationsmassnahmen zuhanden der Anspruchsgruppen im Kontext «Anmeldung üK»	20	0	
Sensibilisierungsmassnahmen für Berufsbildner:innen und üK-Anbieter	20	0	

Realisierungsplan	Aufwand (Personal)		Dritt-kosten
Inkrement #3: Berufsschulzeugnisse als digitale Nachweise	**PT/int**	**PT/ext**	**fällig**
Governance			
Datenarchitektur des dezentralen Datenregister zur Ausstellung von Berufsschulzeugnissen	5	2	
Informationssicherheits- und Datenschutzkonzept (ISDS) für das Inkrement 2	5	2	
Beratung bei den Prozessen der Berufsbildung	20	0	
Architektur			
Technische Infrastruktur und Prozeduren zum Ausstellen von digitalen Zeugnissen	15	40	
Entwicklung, Konfiguration inkl. Zugriffsrechte der Agenteninfrastruktur	10	20	
Onboarding der bestehenden Applikationen	0	0	
Integration in die administrativen Abläufe der Geschäftsstelle	10	0	
Technische und organisatorische Massnahmen im Bereich Informationssicherheit und Datenschutz	15	5	
Qualitätsmanagement, Testing und Validierung	10	15	
Management			
Projektmanagement (inkl. Risikomanagement)	15	0	
Administration und Support (z. B. HR, Buchhaltung etc.)	10	0	
Betrieb			
Laufende technische Betriebskosten (pro rata)	0	60	X
Betrieb der Geschäftsstelle	51	0	
Begleitmassnahmen			
Technische Spezifikation für die Controller und deren Agenten	10	5	
Unterstützung der Berufsfachschulen bei der Anpassung der Ausstellungsprozesse	20	0	
Kommunikationsmassnahmen zuhanden der Anspruchsgruppen im Kontext «Berufsfachschulzeugnisse»	20	0	
Sensibilisierungsmassnahmen für die Verantwortlichen der Berufsfachschulen	20	0	

Realisierungsplan	Aufwand (Personal)		Drittkosten
Inkrement #4: Erteilen Bildungsbewilligung	**PT/int**	**PT/ext**	**fällig**
Governance			
Datenarchitektur des dezentralen Datenregisters zum Erteilen der Bildungsbewilligung	5	2	
Informationssicherheits- und Datenschutzkonzept (ISDS) für das Inkrement 2	5	2	
Beratung bei den Prozessen der Berufsbildung	15	0	
Architektur			
Technische Infrastruktur und Prozeduren zum Erteilen von digitalen Bildungsbewilligungen	10	25	
Integration in die administrativen Abläufe der Geschäftsstelle	10	0	
Technische und organisatorische Massnahmen im Bereich Informationssicherheit und Datenschutz	10	5	
Qualitätsmanagement, Testing und Validierung	7.5	10	
Management			
Projektmanagement (inkl. Risikomanagement)	12	0	
Administration und Support (z. B. HR, Buchhaltung etc.)	8	0	
Betrieb			
Laufende technische Betriebskosten (pro rata)	0	40	X
Betrieb der Geschäftsstelle	51	0	
Begleitmassnahmen			
Technische Spezifikation für die Controller und deren Agenten	5	5	
Unterstützung der Berufsbildungsämter bei der Anpassung der Ausstellungsprozesse	20	0	
Kommunikationsmassnahmen zuhanden der Anspruchsgruppen im Kontext «Bildungsbewilligung»	20	0	

5.2 Begleitmassnahmen zur Realisierung des Konzepts

Ein wesentliches Merkmal der Projektplanung ist der Einbezug von Begleitmassnahmen, um die nachhaltige Wirkung der Inkremente zu gewährleisten. Dies setzt voraus, dass der angestrebte Nutzen ermittelt wird und die dafür erforderlichen Treiber identifiziert werden. Typische Massnahmen sind die Dokumentation von Schnittstellen, die Schulung derjenigen, die die Datenföderation nutzen sowie Kommunikationsmassnahmen. Es muss festgelegt werden, wer für die Durchführung der Massnahmen verantwortlich ist, und es muss sichergestellt werden, dass diese Personen für deren Wirksamkeit Rechenschaft ablegen. Hierbei handelt es sich um eine Governance-Aufgabe. Oft unterliegen diese Begleitmassnahmen einer geteilten Verantwortung, die politischen Willen und das Engagement der Führungskräfte erfordert.

6. Kosten und Finanzierung des Realisierungsplans

Die Schätzung der Kosten ist mit einer gewissen Unsicherheit behaftet. Die wichtigsten Kostenfaktoren und die Kostendynamik eines solchen Vorhabens können basierend auf vergleichbaren Infrastrukturprojekten im Bildungsbereich bestimmt werden. Zudem werden Annahmen zur Kostenstrategie getroffen (beispielsweise durch eine Cloud-First-Strategie, wo vor allem Betriebs- anstatt Investitionskosten eine Rolle spielen). Die Kostenschätzung für die Umsetzung bezieht sich auf einen Entwicklungsbereich, der sich mit der Bereitstellung neuer Funktionalitäten (zusammen mit den entsprechenden Begleitmassnahmen) befasst, sowie auf einen Betriebsbereich, der die Geschäftsstelle und den technischen Betrieb umfasst. Erstere sind in der Regel einmalig und variabel und zeigen die umzusetzenden Anforderungen an die Funktionalität. Letztere bleiben relativ stabil und steigen mit einer zunehmenden Nutzung der Datenföderation leicht an. Nebenkosten, wie sie zum Beispiel durch Integrationsmassnahmen entstehen, werden in diesem Kostenmodell nicht berücksichtigt, da sie von den Mitgliedern (z. B. Lehrbetriebe, OdAs etc.) zu tragen sind.

6.1 Kostenrechnungsmodell der Datenföderation

Die folgende Abbildung veranschaulicht die Grundprinzipien des Kostenrechnungsmodells der Datenföderation. Der Kostenplan der Geschäftsstelle basiert auf dem klassischen Kontenrahmen einer Organisation in der Schweiz.

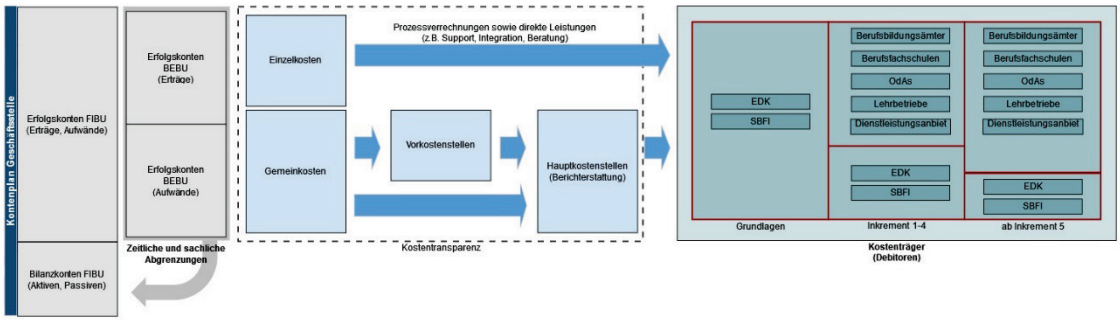

Abbildung4: Kostenrechnungsmodell der Datenföderation

Folgende Bemerkungen sind für die Handhabung der Kosten der Datenföderation relevant:

- Die Kostenträger spiegeln die Finanzierung der Datenföderation wider und nicht die Kostenrechnung ihrer Dienstleistungen. Die Berichtserstattung für die Steuerung erfolgt mittels der Hauptkostenstellen, das heisst Governance, Geschäftsstelle, Betrieb. Aus diesem Grund sind die Kostenträger in diesem Modell den Debitoren (der Verrechnungsseite) gleichgestellt. Die Finanzierung wird weiter unten ausführlicher beschrieben (s. Kapitel 6.3).
- Einzelkosten sind mehrheitlich direkt zuweisbar und variabel. Aus diesem Grund werden sie in der Regel über kostenpflichte Prozesse (z. B. Supportleistungen, Integration etc.) oder sonstige Leistungen (z. B. Beratung) gehandhabt. Solche Kosten werden den Kostenträgern (d. h. Debitoren) direkt verrechnet.

- Gemeinkosten sind relativ fixe Kosten, die von allen getragen werden müssen. Sie werden in zwei Unterkategorien aufgeteilt:
    - Vorkostenstellen sind indirekte Kosten, die nicht direkt mit der Erbringung von Leistungen assoziiert sind (z. B. Management, Kommunikation, Rechtsberatung etc.). Solche Kosten werden unter der Hauptkostenstelle auf eine und für alle vereinbarte und gleiche Basis verteilt. Diese Aufteilung von (indirekten nicht produktiven) Kosten ist weiter unten beschrieben.
    - Hauptkosten dagegen sind indirekte Kosten, die aber durch eine unmittelbare Beteiligung an der Datenföderation verursacht werden (z. B. Administration, Nutzung der Infrastruktur etc.). Diese Kosten werden auf einer fairen Kostenverteilungsbasis (d. h. Umlageschlüssel) auf alle Kostenträger, wie weiter unten beschrieben, verteilt. Dabei ist zu beachten, dass die Umlageschlüssel je nach Hauptkostenstelle unterschiedlich sein können.
- Gemeinkosten lassen sich am besten durch Betriebsausgaben anstatt Investitionsausgaben verwalten. So wäre es beispielsweise sinnvoll, für das Hosting von Knoten und Agenten eine Cloud-Beschaffung in Betracht zu ziehen.
- Sachliche Abgrenzungen aus der Betriebsbuchhaltung (BEBU) beinhalten beispielsweise Steuern, Abschreibungen, kalkulatorische Zinsen usw. und werden wie üblich im Sinne. der Finanzbuchhaltung (FIBU) abgegrenzt.

6.2 Realisierungs- und Betriebskosten

Über drei Jahre hinweg belaufen sich die Gesamtkosten auf rund 4,3 Millionen Franken. Dies entspricht einem durchschnittlichen Betriebskapital von 120'000 Franken pro Monat. In der Praxis liegen allerdings die Entwicklungs- und Betriebskosten im Durchschnitt unter 1 Million Franken pro Jahr. Im ersten Jahr werden die Grundlagen für alle weiteren Inkremente geschaffen, so dass hier die Betriebskosten über einer Million liegen. Dies liegt unter anderem darin begründet, dass zu Beginn Governance-Kosten anfallen, die sich in den nachfolgenden Inkrementen deutlich verringern. Die Kostenanalyse – hier in zusammengefasster Form – geht davon aus, dass die Realisierung, schrittweise mittels Inkremente erfolgen wird. Durch Lerneffekte werden Kostensynergien erzielt.

Gemäss Realisierungsplan werden die Kosten in Kategorien eingeteilt (z. B. Governance, Architektur, Betrieb usw.). Jedes Inkrement zieht auch einen anderen architektonischen Schwerpunkt und damit verbundene Begleitmassnahmen nach sich, die sicherstellen sollen, dass die neue Funktionalität richtig verstanden und angewendet wird. Zuletzt gibt es aufgrund dieses inkrementellen Vorgehens eine stabile Entwicklung der Betriebskosten.

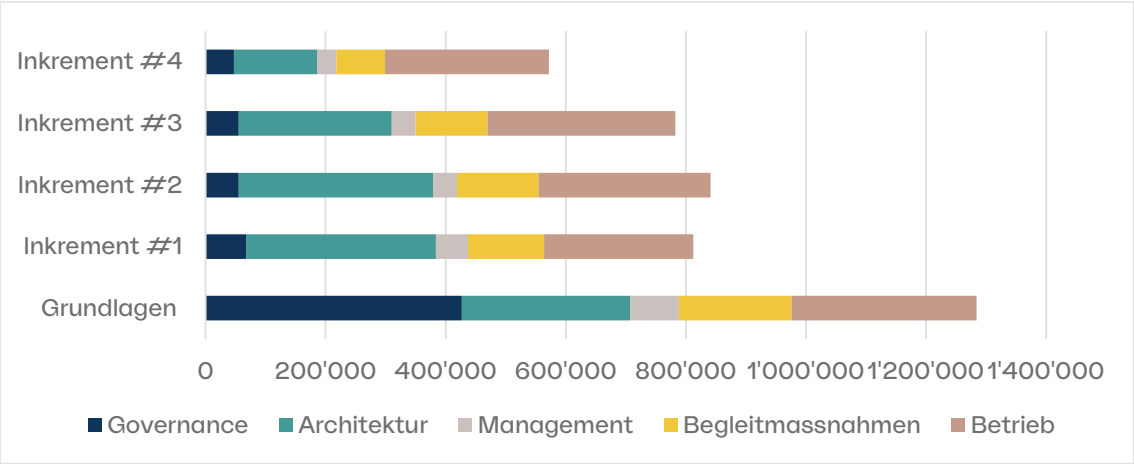

Abbildung 5: Kosten nach Projektphase

Die Geldflussrechnung, die sich aus den Entwicklungskosten und den wiederkehrenden Betriebskosten zusammensetzen, ist für die Zeitdauer bis und mit Inkrement 4 gesondert erfasst und weist einen relativ stabilen Geldfluss auf. Dieser lässt sich leicht in die Budgetzyklen der Träger der Datenföderation einfügen.

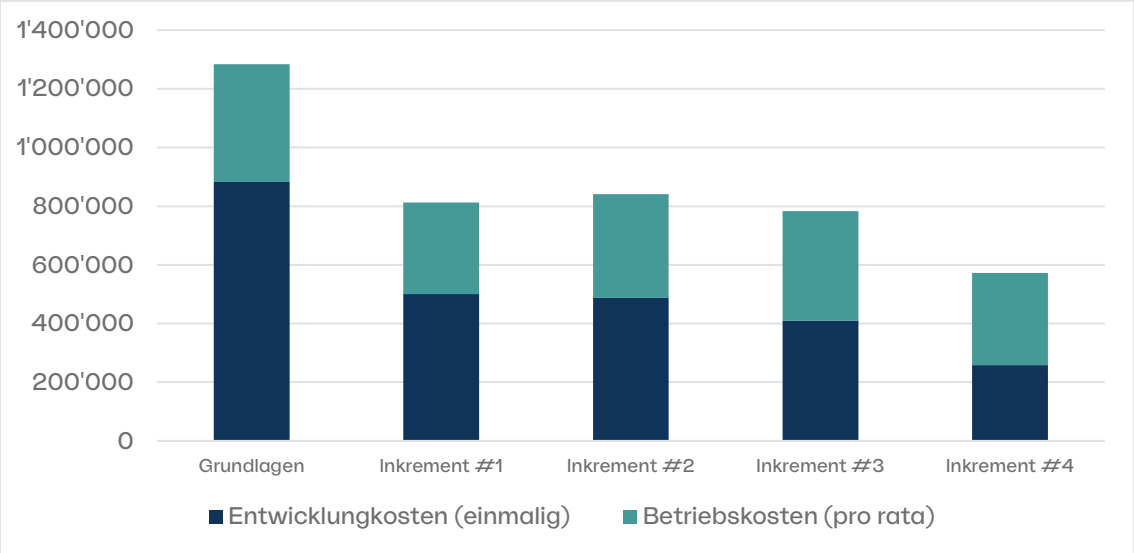

Abbildung 6: Geldflussrechnung gemäss Inkrement

Tabelle 4a: Gesamtkosten Realisierung der Datenföderation **(Grundlagen, Inkremente 1-4)**

	CHF (exkl. MwSt)
Governance	652'600
Architektur	1'314'500
Betrieb	1'428'800
Management	245'700
Begleitmassnahmen	651'900
Gesamtkosten	*4'293'500*

Tabelle 4b: Aufteilung der Gesamtkosten nach Projektphasen (Grundlagen und Inkremente 1-4)

	geschätzte Zeitdauer	CHF (exkl. MwSt)
Grundlagen	**6 Monate**	
Governance		426'900
Architektur		280'300
Betrieb		307'900
Management		81'400
Begleitmassnahmen		187'600
Zwischensumme		*1'284'100*
Inkrement #1: Ausstellung EFZ als digitaler Nachweis	**6 Monate**	
Governance		67'400
Architektur		316'200
Betrieb		248'700
Management		53'700
Begleitmassnahmen		126'700
Zwischensumme		*812'700*
Inkrement #2: Anmeldung zum üK	**6 Monate**	
Governance		55'400
Architektur		324'100
Betrieb		286'200
Management		39'500
Begleitmassnahmen		136'200
Zwischensumme		*841'400*

Inkrement #3: Berufsfachschulzeugnisse als digitale Nachweise	**6 Monate**	
Governance		55’400
Architektur		254’700
Betrieb		313’000
Management		39’500
Begleitmassnahmen		120’400
Zwischensumme		*783’000*
Inkrement #4: Erteilen Bildungsbewilligung	**4 Monate**	
Governance		47’500
Architektur		139’200
Betrieb		273’000
Management		31’600
Begleitmassnahmen		81’000
Zwischensumme		*572’300*

Tabelle 5: Geldflussrechnung der Datenföderation

	Entwicklungs-kosten (einmalig)	**Betriebskosten pro rata)**
	CHF	**CHF**
1. Jahr		
Grundlagen	882’400	401’700
Inkrement #1: Ausstellung EFZ als digitaler Nachweis	500’650	312’050
2. Jahr		
Inkrement #2: Anmeldung zum üK	487’100	354’300
Inkrement #3: Berufsfachschulzeugnisse als digitale Nachweise	409’800	373’200
3. Jahr		
Inkrement #4: Erteilen Bildungsbewilligung	258’800	313’500

6.3 Finanzierung durch die Kostenträger

Im vorliegenden Konzept wird ein dreistufiges Finanzierungsmodell der Datenföderation vorgeschlagen (s. Abbildung 4 in Kapitel 6.1):

1. Grundlagen: Die Realisierungskosten werden je hälftig von EDK und SBFI getragen. Angenommen wird, dass die Kosten seitens EDK gemäss EDK-Schlüssel unter den Kantonen aufgeteilt werden.
2. Inkremente 1–4: In dieser ersten Betriebsphase werden Einzelkosten den Parteien in Rechnung gestellt, die Unterstützung bei der Konzeption, Entwicklung und Integration ihrer Lösungen anfordern. Sonstige Gemeinkosten (die dem grössten Teil der Kosten entsprechen) werden analog zur Finanzierungsstufe 1 von EDK und SBFI je hälftig getragen.
3. Ab Inkrement 5: In der weiteren Betriebsphase werden Einzelkosten wie bisher verrechnet. Zudem werden jene Anteile der Gemeinkosten, die im Rahmen von Betrieb und Wartung der technischen Infrastruktur und den sonstigen täglichen Aufgaben der Geschäftsstelle entstehen, unter den Mitgliedern aufgeteilt. Es ist den Kantonen einzeln überlassen, ob ihre Einrichtungen (z. B. Berufsbildungsamt, Berufsfachschulen) zu verrechnen sind oder ob der Kanton alle aggregierten Kosten übernehmen will. In jedem Fall werden transkantonal tätigen Organisationen ihre Teilnahme an der Datenföderation direkt in Rechnung gestellt, wobei es ihnen freisteht, entsprechende Vereinbarungen mit einzelnen Kantonen zu treffen. Eine deutlich reduzierte finanzielle Beteiligung der EDK und des SBFI ist nach wie vor vorhanden. Sie beschränkt sich aber auf Nebenleistungen, die zur Gewährleistung einer angemessenen Governance erforderlich sind (z. B. bildungspolitische Steuerung, Risikomanagement, Audit etc.).

7. Risikomanagement der Datenföderation

Die folgende Analyse berücksichtigt Risiken, die sich entweder im Rahmen des Projekts oder später im Betrieb manifestieren könnten. Dementsprechend besteht der Ansatz nicht nur durch den proaktiven Einsatz von Techniken des Projektrisikomanagements, sondern auch in der Berücksichtigung notwendiger operativer Risikomanagementansätze (z. B. die Nutzung von IT-Kontrollen zur Bewältigung von Sicherheitsrisiken). Aufgrund ihrer Relevanz wurden potenzielle Risiken vor allem aus den Bereichen Technologie, Recht und Innovation identifiziert und analysiert. Diese Bereiche werden verwendet, um Massstäbe (d. h. klein, mittel, gross etc.) zu definieren, anhand derer die potenziellen Auswirkungen von Risiken eingeordnet werden können. Dadurch wird sichergestellt, dass die Bewertung von unterschiedlichen Risiken möglichst kohärent durchgeführt werden kann. Entsprechend wurden Massnahmen definiert, um die identifizierten Risiken zu behandeln. Diese Analyse der Risiken erfolgte durch die interne Arbeit während der Konzeptionsphase sowie durch Gespräche mit Vertreterinnen und Vertretern der in der beruflichen Grundbildung beteiligten Akteursgruppen. Risikomanagement ist ein kontinuierlicher Prozess welche die Identifizierung neuer Risiken sowie die Neubeurteilung bestehende Risiken erfordert. Die vorliegende Risikoanalyse, welche in Form eines Risikoregisters (s. Tabelle 7) zusammengefasst ist, gilt somit nicht als abschliessend.

Alle Risiken werden in einem Risikoregister erfasst, wozu ein Risikoprofil eine einfache visuelle Zusammenfassung liefert. Die Risikomatrix ist in farblich gekennzeichnete Bereiche unterteilt, von denen jeder eine andere Strategie zur Risikobewältigung widerspiegelt. Im roten

Bereich befinden sich jene Risiken, die als inakzeptabel gelten und wofür Massnahmen ergriffen werden müssen. Die im gelben Bereich befindlichen Risiken unterliegen einer ständigen aktiven Überwachung. Oft sind bereits Massnahmen im Einsatz, die die Auswirkungen oder Wahrscheinlichkeit jener Risiken verringern sollen. Somit muss lediglich sichergestellt werden, dass diese Massnahmen tatsächlich wirksam sind. Die Risiken im grünen Bereich gelten im Allgemeinen als akzeptabel oder werden angemessen gehandhabt, so dass sie nur dann neu bewertet werden müssen, wenn die Umstände darauf hindeuten, dass sich ihr Risikoniveau geändert hat.

Zu den wichtigsten Risiken gehören diejenigen, die mit der Zurückhaltung gegenüber neuen Innovationen verbunden sind. Dies darin, da man nicht voraussehen kann, was sie in Zukunft bringen werden oder da man selber nicht über die nötigen Fachkenntnisse verfügt, um sie zu verstehen (z. B. Risiken *#2*, *#3* und *#6* im Risikoregister, s. unten). Dies kann wiederum die Suche nach einem Konsens über die beste Vorgehensweise verlangsamen (z. B. Risiken *#5* und im Risikoregister). Solche Hemmungen sind unvermeidlich, da die Folgen von Innovationen oft erst nach langer Zeit sichtbar werden. Dies kann nur durch einen offenen Dialog und die Bereitschaft, Veränderungen zu akzeptieren, geschehen.

Eine weitere grosse Risikoquelle sind unbekannte Sicherheitslücken oder solche, die sich aus der Art und Weise ergeben, wie die Komponenten der Datenföderation (z. B. Controllers, Agenten) entwickelt werden (z. B. Risiken *#7*, *#9*, *#10*, *#11* und *#19* im Risikoregister). Dies ist eine häufige Risikokategorie bei IT-Projekten, wofür es verschiedene ausgereifte Ansätze gibt, von denen der Einsatz eines Informationssicherheitsmanagementsystems (ISMS) einer der gängigsten ist. Andererseits kann Datenschutzrisiko weitgehend eingedämmt werden, da keine personenbezogenen Daten in der Blockchain gespeichert werden, auch wenn andere sekundäre Formen des Risikos immer noch von ausserhalb der Datenföderation ausgehen können (z. B. Risiko *#15* im Risikoregister).

Andere, eher isolierte Risiken sind im Risikoregister zu finden, das wiederum durch eine gründliche Analyse und Untersuchung anhand der verfügbaren Informationen gestützt wird. Es ist jedoch anzumerken, dass eine detailliertere Risikobewertung erst möglich ist, wenn der politische Wille seine Präferenz für bestimmte Architekturentscheidungen zum Ausdruck gebracht hat.

7.1 Auflistung der Risiken

Die nachfolgende Matrix visualisiert die Verteilung von verbleibenden Restrisiken nach Risikoeignern. Das heisst sie stellt die geschätzte Schadensauswirkung und Eintrittswahrscheinlichkeit der identifizierten Risiken dar, unter der Annahme, dass alle in Tabelle 7 vorgeschlagenen Massnahmen umgesetzt wurden. Aus Gründen der Übersichtlichkeit werden Risikoeignern in zwei Gruppen zusammengefasst:

1. Einen Teil der Risiken betreffen Gefahren für den Aufbau und Betrieb der technischen Infrastruktur der Datenföderation. Für die Überwachung und Minimierung dieser Risiken sind die Betreiber der Infrastruktur sowie die Geschäftsstelle verantwortlich.

2. Weitere Risiken betreffen neben Gefahren für die technischen Infrastrukturen von Mitgliedern und Teilnehmenden der Datenföderation vor allem Herausforderungen, die die Umsetzung der Datenföderation auf nicht-technischer Ebene bedrohen. Monitoring und Bekämpfung dieser Risiken obliegen den betroffenen Akteuren sowie der bildungspolitischen Steuerung.

Die Nummerierung der Risiken in der Abbildung entspricht der Nummerierung der Risiken in Tabelle 7. Die Abbildung verdeutlicht, dass Restrisiken bestehen bleiben, selbst wenn zentrale Massnahmen zur Risikominimierung ergriffen und umgesetzt wurden. Eine kontinuierliche Überwachung der bekannten Risiken und ein Screening auf bisher nicht erkannte Risiken bleiben daher notwendig.

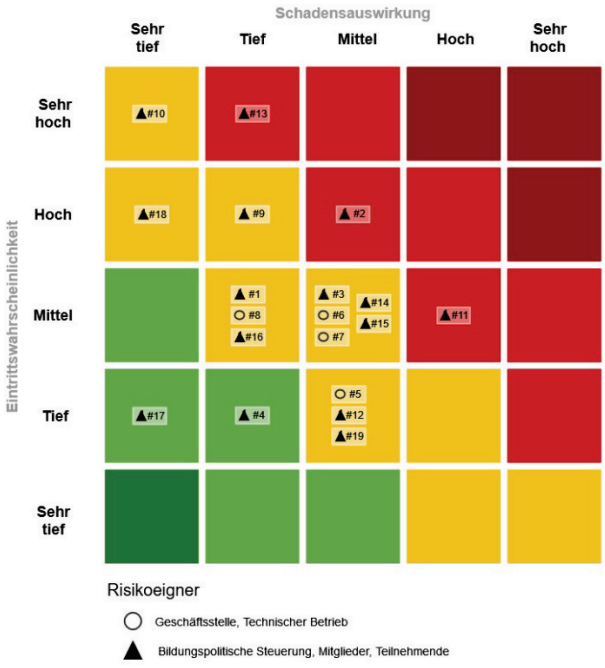

Abbildung 7: Risikomatrix nach Eignern

In Tabelle 6 sind die Risiken mit Titel, Risikoeigner, Auswirkung, Wahrscheinlichkeit, Massnahmen, Restauswirkung und Restwahrscheinlichkeit ausformuliert. Unter den Risikoeignern werden die Akteure genannt, bei welchen das Risiko zu verorten ist (s. Kapitel 3.1 im Teil 2 des Konzepts). Die Datenföderation hat auf einige Risiken nur begrenzten oder keinen Einfluss. Es ist wichtig, dass jeweils die betreffenden Akteure die Massnahmen zur Risikominimierung formulieren, ergänzen und umsetzen.

Tabelle 6: Risikoanalyse

Nr.	Beschreibung	Risikoeigner	Auswirkung	Wahrscheinlichkeit	Massnahmen	Restauswirkung	Restwahrscheinlichkeit
Innovation							
1	Potentielle Mitglieder lehnen es ab, sich der Datenföderation anzuschliessen, so dass die Datenföderation ihr Potenzial nicht entfalten kann.	Mitglieder Techn. Betrieb	mittel	sehr hoch	Vertrauensmassnahmen durch Kommunikation, Pilotprojekte und weitere Massnahmen.	tief	mittel
2	Die Kantone zögern bei der Umsetzung der Datenföderation, da die Auswirkungen auf das bestehende System unklar sind.	Diverse	hoch	hoch	Erstellen einer Planungsübersicht betreffend den bestehenden Fachapplikationen, Anleitungen zur Integration und weiterer Massnahmen.	mittel	hoch
3	Es kommt zu Widerständen durch die Kantone wegen sich verändernder Rollen, Aufgaben und Verantwortlichkeiten.	Bildungspolitische Steuerung	sehr hoch	hoch	Informationen, Leitfäden, Handbücher	mittel	mittel
4	Fehlendes Fachwissen und fehlende Ressourcen bei allen Mitgliedern führen zu einer Verzögerung bei der Umsetzung.	Mitglieder	mittel	mittel	Unterschiedliche Unterstützungsmassnahmen für die Integration, wie beispielsweise Anleitungen und Schulungen und weitere Massnahmen.	tief	tief
5	Aufgrund des frühen Entwicklungsstands der Technologie ist noch nicht klar welche technischen Standards sich durchsetzen werden.	Geschäftsstelle	hoch	mittel	Bei der Suche nach einer technischen Lösung fand eine Orientierung an bereits bestehenden Systemen statt. Regelmässiger Austausch mit öffentlichen und privaten Stellen, die ähnliche Projekte verfolgen.	mittel	tief

Technologie							
6	IT-Unternehmen verfügen über nur beschränktes technisches Wissen zur Umsetzung einer Datenföderation.	Techn. Betrieb	mittel	mittel	Beobachtung des SSI-Ökosystems sowie regelmässige Austausche mit dem Bund, um sicherzustellen, dass die Berufsbildung und der Bund in Zukunft nicht jeweils ihr eigenes Blockchain Netzwerk betreiben.	mittel	mittel
7	Die Blockchain-Infrastruktur erweist sich als unsicher.	Techn. Betrieb	mittel	hoch	Einführung eines ISMS und Durchführung regelmässiger Updates & Upgrades um die Sicherheit zu gewährleisten. Periodische Überprüfung von Schwachstellen inkl. entsprechender Massnahmen. Überwachung und Überprüfung mittels Übersicht der aktuellen Cyber-Bedrohungen und Tendenzen.	mittel	mittel
8	Die Skalierbarkeit und Überlastung der Datenföderation ist ungenügend erprobt.	Techn. Betrieb	mittel	mittel	Es wird eine Skalierbarkeitsinfrastruktur mit entsprechender Verwaltung verwendet. Leistungsengpässe werden durch die aufgesetzte Infrastruktur vermieden. Zudem wird mittels Betriebsmonitorring der optimale Einsatz von Ressourcen sichergestellt.	tief	mittel
9	Verletzung der Sicherheit von cloudbasierten Brieftaschen.	Teilnehmende Mitglieder	mittel	hoch	Technische und organisatorische Massnahmen. Für Mitglieder eine Vertragsklausel, die Sicherheitsprüfungen der Mitglieder erlauben. Aufzeigen von Alternativen zur cloudbasierten Brieftasche (lokale elektronische Brieftasche als Alternative für Teilnehmende).	tief	hoch
10	Verletzung der Sicherheit von lokalen privaten elektronischen Brieftaschen.	Teilnehmende	sehr tief	sehr hoch	Umfassende Sensibilisierung mittels Kommunikationsmassnahmen sowie automatische Backups ermöglichen.	sehr tief	sehr hoch

11	Verletzung der Sicherheit von organisationsinternen elektronischen Brieftaschen.	Mitglieder	sehr hoch	hoch	Einsatz von Massnahmen zum Schutz der IT-Infrastruktur sowie automatische Backups.	hoch	mittel
12	Fehlende Einigkeit betreffend Standards und Prozessen innerhalb der Datenföderation.	Mitglieder	hoch	mittel	Gemeinsame Einigung zu verbindlichen Standards unter Berücksichtigung von OdA und Lehrbetrieben.	mittel	tief
Recht							
13	Der Ansatz der informationellen Selbstbestimmung lässt sich nicht realisieren.	Teilnehmende	tief	sehr hoch	Einsatz von technischen und organisatorischen Massnahmen zur Durchsetzung des Grundsatzes der informationellen Selbstbestimmung sowie Sensibilisierung aller beteiligten Akteure im Umgang mit dem Grundsatz der informationellen Selbstbestimmung.	tief	sehr hoch
14	Die Teilnehmenden verfügen nicht über die erforderlichen digitalen Kompetenzen zur Durchsetzung ihrer Rechte.	Teilnehmende	hoch	mittel	Einsatz von technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit und -integrität sowie Schutz der Rechte und Freiheiten von (minderjährigen) Personen. Sensibilisierung mittels Kommunikationsmassnahmen zum Umgang mit der informationellen Selbstbestimmung über die eigenen Daten.	mittel	mittel
15	Durch Identitätsinfrastrukturen besteht die Möglichkeit einer Überidentifikation.	Bund Geschäftsstelle	hoch	mittel	Bereitstellung eines Proxy-Identifizierungsdienst, der eine E-ID akzeptiert, jedoch in einen transitiven Identifikator übersetzt, der die Person nicht identifiziert. Kopplungsverbot bei der Teilnahme an der Datenföderation.	mittel	mittel
16	Die Interaktion mit der Datenföderation erfolgt nicht barrierefrei.	Mitglieder	tief	mittel	Anlaufstellen für Personen mit Beeinträchtigungen durch die Ausgabestellen.	tief	mittel

17	Es befinden sich Daten im dezentralen Datenregister, die nicht in das dezentrale Datenregister gehören.	Mitglieder	mittel	mittel	Einsatz von technischen Massnahmen, um zu verhindern das falsche Informationen auf die Blockchain geschrieben werden sowie den Einsatz von sog. Tombstones, welche Inhalte unleserlich machen. Einsatz von Sicherheitsmassnahmen, um zu verhindern, dass persönliche Daten auf der Blockchain oder bei der falschen Person landen. Kontrolle auf Node-Ebene 4-Augen-Prinzip	sehr tief	tief
18	Aufgrund von fehlendem bildungspolitischen Willen können die notwendigen gesetzlichen Grundlagen für den Datenaustausch nicht geschaffen werden.	Bildungspolitische Steuerung	mittel	sehr hoch	Interkantonale Vereinbarung zur Harmonisierung der Daten in der Berufsbildung.	sehr tief	hoch
19	Daten aus der Datenföderation werden durch ein Mitglied rechtswidrig missbraucht.	Geschäftsstelle Mitglieder	mittel	tief	Einsatz von technischen und organisatorischen Massnahmen zur Kontrolle. Zudem Festlegung vertraglicher Massnahmen sowie Sicherheitsaudits und Sensibilisierung mittels Kommunikationsmassnahmen.	mittel	tief

8. Zwischenfazit

Im ersten Teil des Konzepts der Datenföderation für die Berufsbildung wurde der Fokus auf die künftige technische Infrastruktur gelegt. Damit wurden die Aspekte der Effizienzsteigerung, der Datenverfügbarkeit und der Anschlussfähigkeit betont. Der zweite Teil des Konzepts beinhaltete eine Sicht auf personenbezogene Daten wie auch eine adäquate Governance. Das Ziel des Data-Governance-Modells des zweiten Teils ist es, allen beteiligten Akteuren der Datenföderation eine kohärente, effektive Nutzung und einen sicheren und gesetzeskonformen Austausch von Daten zu ermöglichen.

Der nun vorliegende dritte Teil beschreibt, den Zeitrahmen, die Kostenrechnung sowie die Reihenfolge der Umsetzung der Inkremente für die Realisierung des Konzepts der Datenföderation. Zudem wird das Potential der Datenföderation anhand eines nächsten Anwendungsfalls detailliert ausgeleuchtet: der direkte und automatisierte Datenaustausch zwischen Berufsbildungsamt, üK-Anbietern und Lehrbetrieben. Der dritte Teil schliesst mit einer detaillierten Risikoanalyse für die Realisierungsphase.

Gemäss diesem vorliegenden dritten Teil dauert die Realisierung der Datenföderation für die Berufsbildung rund zwei bis drei Jahre. Bereits im ersten Jahr der Realisierung kann in einen Betriebsmodus gewechselt werden. Der weitere Aufbau der Datenföderation erfolgt sodann inkrementell. Die Mehrwerte für die Akteure der beruflichen Grundbildung werden etappiert bereitgestellt. Dieser Ansatz hat positive Auswirkungen auf den zeitlichen Finanzierungsbedarf. Während zu Beginn der Realisierung die Entwicklungskosten dominieren, nehmen diese mit der Zeit ab. Gleichzeitig steigt der Anteil der Betriebskosten im Zusammenspiel mit den zunehmenden Nutzungszahlen der Datenföderation. Der Realisierungsplan wird ergänzt mit einer Analyse zum Regulierungsbedarf für die Datenföderation und einer Risikoanalyse.

Anhang

Begrifflichkeiten

Begriff	Definition
Agent	Ein Agent ist eine Softwarekomponente, die die Anweisungen eines oder mehrerer Controller verarbeitet, entsprechend in der Datenföderation weiterverbreitet, mit den Knoten kommuniziert oder digitale Nachweise (und damit personenbezogene Daten) speichert.
Ausgabestelle	Unter einer Ausgabestelle («Issuer») versteht man eine Stelle, die z. B. durch eine staatliche Institution autorisiert ist, digitale Nachweise auszustellen.
Autoritative Quelle	Datenquellen, die ein hohes Mass an Glaubwürdigkeit und Vertrauen besitzen.
Betreiber:in	Dies können Institutionen, private oder juristische Personen sein, die Knoten betreiben.
Blockchain	Ein Ledger-Speichersystem, bei dem Transaktionsdaten angehängt werden und nicht nachträglich geändert werden dürfen. Blockchains werden durch ein Netzwerk von Knoten realisiert und sind daher in der Regel dezentralisiert.
Controller	Unter Controller versteht man eine Software-Komponente, die es Personen und Institutionen ermöglicht, über eine Benutzeroberfläche auf den Agenten zuzugreifen und so Zugang zu digitalen Nachweisen zu erhalten, das dezentrale Datenregister zu nutzen oder mit anderen Mitgliedern oder Teilnehmenden der Datenföderation zu kommunizieren.
Datenprovenienz	Die Rückverfolgbarkeit bestimmter Daten zu ihren ursprünglichen Quellen. Damit kann beispielsweise festgestellt werden, ob bestimmte Daten tatsächliche von autoritativen Quellen stammen.
Dezentrales Datenregister	Ein dezentrales Datenregister ist ein öffentlich zugänglicher und von allen lesbarer dezentraler Speicher, der alle notwendigen Informationen enthält, um eine Datenföderation im Allgemeinen und ein Ökosystem für digitale Nachweise im Speziellen betreiben zu können.
Dezentrale Identifikatoren (DID)	Eine Form der Identifikation, die in dezentralen Systemen verwendet wird und die Verknüpfung von Ereignissen mit Daten in einer Weise ermöglicht, dass nur die betroffenen Parteien jene Verknüpfungen herstellen können.
Elektronische Brieftasche	Bei einer elektronischen Brieftasche handelt es sich um eine Software-Applikation für die sichere Aufbewahrung digitaler Nachweise.
Informationsdienst (sog. Discovery-Service)	Ein technischer Dienst, der innerhalb des dezentralen Datenregisters die (automatische) Ermittlung von Dienstleistungen, die von Mitgliedern angeboten werden, ermöglicht.
Inhaber:in	Unter Inhaberin oder Inhaber versteht man die Person oder Institution, die einen digitalen Nachweis elektronisch besitzt.

Intelligente Verträge (Smart Contracts)	Intelligente Verträge sind Computerprogramme, die die automatisierte Bearbeitung von Daten und darauf basierend eine automatisierte Entscheidungsfindung entlang von vordefinierten Kriterien bewirken.
Knoten (Node)	Ein Knoten ist eine Verarbeitungsinstanz des dezentralen Datenregisters. Knoten tätigen, überprüfen und speichern Transaktionen auf dem dezentralen Datenregister und können zudem auch intelligente Verträge hosten.
Mitglied	Eine institutionelle Partei der Datenföderation, die aktiv mitwirken darf (z. B. Erstellen von Transaktionen). Solche Parteien müssen mit dem Betreiber der Datenföderation einen Vertrag unterzeichnen.
Nutzungsbedingungen	Metadaten, die auf digitalen Nachweisen zum Zwecke der Regelung der Berechtigungen, Verbote und Verpflichtungen geschrieben werden.
Permissioned (Blockchain)	Eine Blockchain Infrastruktur deren Lese- und Schreibrechte eingeschränkt sind.
Polyzentrische Governance	Ein Governance-Ansatz, bei dem mehrere Parteien innerhalb eines Ökosystems Regeln und Strategien aushandeln, um gemeinsame Probleme zu lösen.
Proof-of-Stake	Ein Verfahren, mit dem ein Blockchain-Netzwerk einen Konsens erreichen kann, oft in dem energieintensive Berechnungen gelöst werden müssen.
Privacy by Default	Die Konzeption eines Systems mit solchen Voreinstellungen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt sind, soweit die betroffene Person nicht etwas anderes bestimmt.
Privacy by Design	Ein Ansatz, mit dem Schutz von Personendaten präventiv bei der technischen und organisatorischen Konzeption eines Systems gewährleistet wird.
Public-Key-Infrastructure	Eine Infrastruktur zur Ausstellung, Verteilung und Validierung von Schlüsselmaterialen, deren Zugehörigkeit zu bestimmten Organisationen bescheinigt wurde.
Schema	Eine Vorlage für einen digitalen Nachweis, welche dessen Inhalt spezifiziert (d. h. Metadaten inkl. Nutzungsbedingungen, Behauptungen, Beweismethode).
Self Sovereign Identity (SSI)	Ein Ansatz für das Identitätsmanagement, bei dem digitale Nachweise verwendet werden, um Attributinformationen über eine Person zu übermitteln (z. B. Name, Vorname, Geburtsdatum).
Software-Architekturrichtlinien	Vom technischen Betrieb festgelegte und durch die Geschäftsstelle genehmigte Richtlinien. Sie bestimmen, wie Software (z. B. Intelligente Verträge) für die Datenföderation zu entwickeln ist (z. B. Vorlagen für Standardabläufe oder Umsetzung der Sicherheitsvorkehrungen etc.).
Teilnehmende	Eine Partei der Datenföderation, die passiv mitwirken darf (z. B. Einsicht von öffentlichen Informationen im dezentralen Datenregister oder die Verifikation von Nachweisen). Solche Parteien müssen mit dem Betreiber oder mit der Betreiberin der Datenföderation in der Regel keinen Vertrag unterzeichnet haben.

Tombstone	Eine fehlerhafte Transaktion auf dem dezentralen Datenregister kann als Tombstone deklariert werden. Die Inhalte der Transaktion sind somit geschwärzt und nicht mehr abrufbar.
Transaktion	Eine Transaktion ist eine Operation, mit der Daten in das dezentrale Datenregister übernommen werden können. Transaktionen beinhalten keine personenbezogenen Daten.
Überprüfer:in	Unter einer Überprüferin oder einem Überprüfer versteht man Personen oder Institutionen, welche die Validität von ihnen vorgelegten digitalen Nachweisen mithilfe der Informationen auf dem dezentralen Datenregister überprüfen.
(verifizierbarer) digitaler Nachweis	Im vorliegenden Kontext beinhaltet ein digitaler Nachweis eine oder mehrere Aussagen einer Institution oder Behörde (z. B. einer Schule oder eines Amtes) zu einem Subjekt (z. B. einer Lernenden). Ob diese Aussagen aus vertrauenswürdiger Quelle stammen, kann mithilfe der Daten auf dem dezentralen Datenregister überprüft werden – daher verifizierbarer digitaler Nachweis.
Zero Knowledge Proof	Ein Zero Knowledge Proof ist ein kryptografisches Protokoll. Es ermöglicht eine Aussage über Daten zu machen, ohne die eigentlichen Daten selbst preiszugeben (z. B. dass man über 18 Jahre alt ist, ohne das Geburtsdatum bekannt geben zu müssen).

Architekturprinzipien

Referenz	Architekturprinzip (AP)
Governance im Sinne der Kontroll- und Steuerungsstrukturen: Dieses Prinzip sorgt dafür, dass sämtliche Datenbewegungen innerhalb der Gesamtarchitektur rechtens sind. Das Prinzip sieht Kontroll- und Steuerungsmechanismen vor, um die Rechtmässigkeit der Datenbewegungen sicherzustellen. Die Governance hat übergeordneten Charakter.	
AP.G.1	**Föderalistische Datenhaltung**: Die Datenföderation kommt ohne zentrale Datenspeicherung aus und ist föderalistisch organisiert. Dabei handelt es sich um einen Zusammenschluss von einzelnen Systemen ist, die ihre jeweilige Selbstständigkeit bewahren.
AP.G.2	**Konsensorientiertes Governance-Modell**: Dient der Akzeptanz und Legitimation der autonomen zugriffsberechtigten Entscheidungsträger. Das Prinzip muss die Agilität und das Funktionieren des Systems fördern, keinesfalls hemmen.
AP.G.3	**Verfügbarkeit von Daten bei Entscheidungsfindungen**: Das Prinzip geht davon aus, dass Entscheidungen erst richtig und rechtens getroffen werden können, wenn sämtliche relevanten Informationen verfügbar sind.
AP.G.4	Transparenz, Integrität und Verantwortlichkeit über bildungsrelevante Ereignisse: Mit diesem Prinzip wird die jederzeitige Revidierbarkeit der Daten gewährleistet. Die Revidierbarkeit der Daten entspringt einem legitimen potenziellen Bedürfnis der betroffenen Person, muss aber klaren Regeln gehorchen.
AP.G.5	**Legitimierter Zugang zur Datenföderation**: Nur wer ein legitimes Interesse an der Föderation hat, bekommt Zugang. Was ein legitimes Interesse ist, muss klar definiert werden. Die Rollen der verschiedenen Teilnehmenden müssen definiert, ihre Rechte im System müssen entsprechend festgehalten werden.
Sicherheit im Sinne des allgemeinen Zustandes, welcher als möglichst frei von (unvertretbaren) Risiken beurteilt wird. Die hier verfolgte Sicherheit ist die objektive Sicherheit (in Abgrenzung zur subjektiven Sicherheit), welche Risiken erkennt, deren Gefährdungspotenzial richtig einschätzt und effektiv entgegenwirkt.	
AP.S.1	**Rollenbasierte Zugangskontrolle (RBAC)**: Damit soll sichergestellt werden, dass nur berechtigte (legitimierte s. AP.G.5) Personen, im Rahmen der ihnen zugeteilten Rollen Zugriff haben bzw. Änderungen vornehmen können.
AP.S.2	**Identitätssicherung der Komponenten**: Der Zugang zur Datenföderation muss auf vertrauenswürdige Teilnehmende beschränkt werden, die in der Lage sein müssen, ihre Identität nachzuweisen. Nur so können die erforderlichen datenschutzrechtlichen Prinzipien eingehalten werden. Bei diesem Architekturprinzip handelt es sich um den allgemeinen Zugang zur Föderation.
AP.S.3	**Identitätssicherung der betroffenen Parteien**: Über die allgemeine Identitätssicherheit des AP.S.2 hinaus, sorgt dieses Architekturprinzip für die bestätigte Legitimation der betroffenen Partei. Diese Zusatzhürde ist wichtig, weil die betroffene Partei gleichsam Eigentümer:in der bearbeiteten Daten ist. Nur sie soll Änderungen (Bearbeitungen) veranlassen dürfen.
AP.S.4	**Kontinuierliches Monitoring der Datenaustausche**: Es werden Instrumente/Mechanismen im System institutionalisiert, welche die Umsetzung der AP.S.1-3 kontinuierlich kontrollieren und sicherstellen. Dieses Architekturprinzip versucht Missbräuche schon im Vorfeld zu erkennen und zu verhindern.

AP.S.5	**Sicherer und rechtskonformer Datenaustausch**: Gemäss diesem Architekturprinzip wird ein technologischer «State of the Art» als Messlatte festgelegt. Damit werden hohe Standards sichergestellt.

Daten im Sinne von Zeichen, die eine Information enthalten. Wichtig in diesem Zusammenhang sind die Informationen, welche Personen im Bildungsbereich betreffen.

AP.D.1	**Daten sind ein gemeinsames Gut im Dienst der Berufsbildung**: Alleinige Eigentümer von Daten in der Bildung sind Lernende. Dieses Prinzip bringt die Notwendigkeit zum Ausdruck, dass Daten in der Bildung nicht von einzelnen Verwaltungsstellen gehortet werden. Sämtliche Bildungsinstitutionen (Lehrbetriebe, Berufsbildungsschulen usw.) stehen im Dienst einer effizienten und zielführenden Datenbearbeitung. Als Ausgabestellen dürfen diese Komponenten dem System keine Hindernisse in den Weg stellen.
AP.D.2	**Datenqualität ist Aufgabe der Komponente**: Eigenverantwortung und datenschutzrechtliche Verantwortlichkeit stehen sich gegenüber. Indem die Komponenten sicher identifiziert werden (AP.S.2–3) und ihnen eine klare Rolle zugeteilt wird (AP.S.1), kann bei Fehlern rasch die Verantwortlichkeit zurückverfolgt werden. Somit muss jede Komponente eigenverantwortlich innerhalb der Föderation handeln.
AP.D.3	**Semantische Interpretierbarkeit der Daten**: Dieses Prinzip sichert die korrekte Interpretation der Informationen (Daten); das Prinzip setzt eine gemeinsame Sprache sowie die jederzeitige Übersetzbarkeit anderslautende Begriffe in die gemeinsame Sprache voraus. Die semantische Interpretierbarkeit der Daten sorgt für Kontinuität, d. h. immer gleiche Bedeutungen der gleichlautenden eingegebenen Daten.

Netzwerk im Sinne. eines Systems mit einer zugrundeliegenden Struktur, welche sich modellieren lässt und die Mechanismen zur Selbstorganisation enthält.

AP.N.1	**Direkter Datenaustausch**: Es ist wichtig, dass die einzelnen Komponenten des Netzwerkes unmittelbar (ohne Mittler) miteinander kommunizieren können. Nur so können sie zeitnah und effizient reagieren. Der direkte Datenaustausch unterstützt auch die Datenintegrität, indem die Datenbearbeitung direkt auf Veranlassung hin erfolgt (ohne Zwischenstufen). Dieses Prinzip setzt voraus, dass die AP.S.1–5 jederzeit eingehalten werden.
AP.N.2	**Atomarität von Bildungsereignissen**: Es ist wichtig Regeln auszudenken und zu implementieren, welche definieren, wann, inwiefern und zu welchem bindenden Zweck Bildungsereignisse offen verkündet werden dürfen. So wird die jederzeitige Aktualität der Daten sichergestellt
AP.N.3	**Asynchronität der Kommunikation**: Wann Daten übermittelt werden, spielt für das Netzwerk keine Rolle; Daten müssen jederzeit für jedermann einsehbar sein. Sobald Daten übergegeben werden, gelten sie.

Quellen zu Kapitel 4. Regulierungsbedarf für die Datenföderation: Interkantonaler Datenaustausch

1. Constitution fédérale (Cst): principalement les articles 47, 48, 48a, 61a, 62, 63;
2. Loi fédérale sur la formation professionnelle (LFPr): principalement l'article 66;
3. Loi fédérale sur la coopération entre la Confédération et les cantons dans l'espace suisse de formation (LCESF): principalement article 1;
4. Convention entre la Confédération et les cantons sur la coopération dans l'espace suisse de formation (CCoop-ESF): principalement article 6a;
5. Chancellerie fédérale, Prise de position du 22 décembre 2011 concernant les bases légales pour la collaboration TIC entre la Confédération et les cantons
6. Convention-cadre de droit public concernant la collaboration en matière de cyberadministration en Suisse 2020
7. Convention-cadre de droit public concernant l'Administration numérique suisse
8. Département fédéral des finances, Rapport explicatif du 11 décembre 2020 concernant la Loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA)
9. Malinvern Giorgio/ Hottelier Michel/ Hertig Randall Maya/ Flückiger Alexandre, les conventions intercantonales in: Droit constitutionnel suisse - Volume I: l'Etat, 2021, pp. 623 - 640.
10. Egli Patricia, art. 47, in: Die schweizerische Bundesverfassung St.Galler Kommentar, 3ème édition, 2014, pp. 991-998.
11. Montavon Michael, Cyberadministration et protection des données - Etude théorique et pratique de la transition numérique en Suisse du point de vue de l'Etat, des citoyen-ne-s et des autorités de contrôle, 2021.
12. Epiney Astrid, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetzte - Aufgezeigt am Beispiel der für Mitarbeiterdaten privater Spitäler massgeblichen gesetzlichen Vorgaben, in: Jusletter 2 mars 2015 www.weblaw.ch