

## 1.1.1

### **Organisationsreglement der Föderation der Identitätsdienste im Bildungsraum Schweiz**

vom 24. Oktober 2019

Die Schweizerische Konferenz der kantonalen Erziehungsdirektoren (EDK),

gestützt auf Artikel 4 des Konkordats über die Schulkoordination vom 29. Oktober 1970 und Artikel 7 des EDK-Statuts vom 3. März 2005,

in Umsetzung der Beschlüsse der EDK-Plenarversammlung zum Ausbau und zur Organisation einer Föderation bestehender und neuer Identity- und Access-Management-Systeme (Rahmenkonzept) vom 26. Oktober 2017, zum Projektauftrag Föderation FIDES – Detailkonzept zur Vorbereitung des Aufbaus vom 22. März 2018 und zur Errichtung der Föderation der Identitätsdienste im Bildungsraum Schweiz vom 24. Oktober 2019, sowie in Umsetzung der EDK-Digitalisierungsstrategie vom 21. Juni 2018 (Ziel 1.3),

beschliesst:

#### **I Allgemeine Bestimmungen**

##### *Art. 1 Geltungsbereich*

Das Reglement regelt Aufbau, Finanzierung, Organisation und Steuerung der Föderation der Identitätsdienste im Bildungsraum Schweiz der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK).

## *Art. 2 Zweck der Föderation*

<sup>1</sup>Die Föderation ist der Zusammenschluss von im Bildungsraum Schweiz aktiven Identitäts-Management-Systemen mit dem Ziel,

- a. den Kantonen und deren Gemeinden die Steuerung und Koordination der Nutzung von digitalen Diensten zu erlauben,
- b. mittels Föderierung der digitalen Bildungsidentitäten einen digitalen Vertrauensraum zu schaffen,
- c. den vereinfachten Zugang zu digitalen Diensten sicherzustellen und damit
- d. Schülerinnen und Schülern sowie Lehrpersonen der Schulen (Primarstufe, Sekundarstufe I, Sekundarstufe II) und der beruflichen Grundbildung sowie dem Personal der kantonalen Bildungsverwaltungen den sicheren Zugang zu digitalen Diensten zu ermöglichen.

<sup>2</sup>Die Föderation bildet eine Schnittstelle zwischen Identitäts- und Dienstleistungsanbietern.

<sup>3</sup>Jeder Kanton schafft die für die Nutzung der Föderation im Kanton notwendigen rechtlichen und organisatorischen Voraussetzungen.

## *Art. 3 Mitglieder der Föderation*

<sup>1</sup>Mitglieder der Föderation sind die vom Kanton bestimmten Identitätsanbieter.

<sup>2</sup>Die Identitätsanbieter erklären nach dem für sie massgebenden kantonalen Recht den Willen zum Beitritt zur Föderation. Der formale Beitritt erfolgt mit Abschluss des Föderationsvertrages.

## II Organisation

### *Art. 4 Grundsatz*

<sup>1</sup>Die Verantwortung für die Föderation liegt bei der EDK. Sie überträgt die strategischen und operativen Aufgaben an

- a. die Steuergruppe Föderation und
- b. die Geschäftsstelle Föderation.

<sup>2</sup>Der technische Betrieb der Föderation wird im Rahmen eines an Dritte zu vergebenden Dienstleistungsauftrags sichergestellt.

### *Art. 5 EDK-Plenarversammlung*

Die Plenarversammlung der EDK hat insbesondere die Aufgaben,

- a. das Organisationsreglement zu erlassen,
- b. das Budget und die Jahresrechnung der Föderation zu genehmigen,
- c. den Jahresbericht der Föderation zur Kenntnis zu nehmen,
- d. die Leistungsvereinbarung mit der Geschäftsstelle Föderation zu genehmigen,
- e. über die Vergabe des technischen Betriebs zu entscheiden und
- f. über die Verwendung der Schnittstelle im Sinne von Artikel 2 Absatz 2 zu entscheiden.

### *Art. 6 Steuergruppe Föderation*

<sup>1</sup>Die Konferenz der Departementssekretäre KDS oder ein von ihr eingesetzter Ausschuss bildet als Steuergruppe das strategische Organ der Föderation.

<sup>2</sup>Zu spezifischen Fragen kann die Steuergruppe Vertretungen des LCH/SER, des VSLCH/CLACESO oder des Staatssekretariats für Bildung, Forschung und Innovation (SBFI) als Gäste an ihre Sitzungen einladen.

<sup>3</sup>Ein Mitglied der Geschäftsstelle Föderation nimmt in beratender Funktion an den Sitzungen der Steuergruppe teil.

<sup>4</sup>Die Steuergruppe hat insbesondere die Aufgaben,

- a. die Föderation entsprechend den Beschlüssen der Plenarversammlung der EDK zu gewährleisten,
- b. die Steuerung der Geschäftsstelle sicherzustellen,
- c. das Budget, die Jahresrechnung und den Jahresbericht der Föderation zuhanden der Plenarversammlung zu verabschieden,
- d. ein externes Finanzcontrolling einzusetzen,
- e. die Leistungsvereinbarung mit der Geschäftsstelle Föderation abzuschliessen,
- f. den Austausch mit den Identitäts- und Dienstleistungsanbietern auf strategischer Ebene sicherzustellen und
- g. die politische und strategische Kommunikation über die Föderation zu verantworten.

#### *Art. 7 Geschäftsstelle Föderation*

<sup>1</sup>Die Gesamtverantwortung für die operative Führung und die Verwaltung der Föderation liegt bei der Geschäftsstelle.

<sup>2</sup>Die Geschäftsstelle hat insbesondere die Aufgaben,

- a. Föderationsverträge mit Identitäts- und Dienstleistungsanbietern abzuschliessen,
- b. technische Dienstleistungen zur Gewährleistung der Schnittstellenfunktion zu erbringen,
- c. den technischen Betrieb der Föderation im Rahmen von Auftragsbearbeitungsverträgen und Service Level Agreements mit Dritten sicherzustellen,
- d. Entscheidungen in Bezug auf die Informationssicherheit und den Datenschutz zu treffen,
- e. die Kommunikation innerhalb der Föderation sicherzustellen,
- f. der Steuergruppe notwendige Entwicklungen in der Architektur der Föderation zu unterbreiten und
- g. der Steuergruppe regelmässig über die laufenden Aktivitäten zu berichten.

<sup>3</sup>Die Steuergruppe schliesst mit der Geschäftsstelle eine Leistungsvereinbarung ab, in der die operativen Ziele der Föderation, die Leistungskriterien, die Aufsicht und die Berichterstattung definiert sind.

<sup>4</sup>Die Föderationsverträge zwischen der Geschäftsstelle und den Föderationsmitgliedern enthalten insbesondere Regelungen zum Betrieb der Föderation.

### **III            Datennutzung und Datenschutz**

#### *Art. 8    Grundsatz*

Die Föderation und deren Geschäftsstelle stellen sicher, dass die Nutzung der personenbezogenen Daten (Attribute) der Umsetzung des in Artikel 2 definierten Zwecks dient, dafür geeignet ist und dabei dem Grundsatz der Verhältnismässigkeit Rechnung getragen wird.

#### *Art. 9    Datenbearbeitungsverantwortung*

Die Geschäftsstelle bearbeitet im Rahmen des Föderationsvertrages Attribute für die beigetretenen Identitätsanbieter. Die Verantwortung für die Attribute verbleibt bei den Identitätsanbietern.

#### *Art. 10   Datenbearbeitungszweck*

Die Geschäftsstelle bearbeitet im Sinne von Art. 2 als Schnittstelle zwischen Bildungsinstitutionen im Bildungsraum Schweiz und Dienstleistungsanbietern im Bildungsbereich Attribute, insbesondere um

- a. in den Kantonen und deren Gemeinden die Koordination und Steuerung der Nutzung von digitalen Diensten zu verbessern und sie bei der Einrichtung eines einfachen und sicheren Zuganges zu Online-Diensten zu unterstützen,
- b. mittels Föderierung der digitalen Bildungsidentitäten einen digitalen Vertrauensraum und rechtliche Sicherheit für die

- Zusammenarbeit von Identitätsanbietern mit Dienstleistungsanbietern zu schaffen,
- c. Schülerinnen und Schülern sowie Lehrpersonen der Schulen (Primarstufe, Sekundarstufe I, Sekundarstufe II) und der beruflichen Grundbildung sowie dem Personal der kantonalen Bildungsverwaltungen den vereinfachten und sicheren Zugang zu digitalen Diensten zu ermöglichen.

*Art. 11 Art und Weise der Datenbearbeitung*

<sup>1</sup>Die Geschäftsstelle erbringt technische Dienstleistungen zur Gewährleistung der Schnittstellenfunktion. Sie zieht für den technischen Betrieb der Föderation Dritte bei.

<sup>2</sup>Die Geschäftsstelle setzt bei der Durchführung der Arbeiten nur Personal ein, das zur Vertraulichkeit verpflichtet worden ist und mit den relevanten Bestimmungen zum Datenschutz vertraut gemacht wurde. Die Geschäftsstelle und jede ihr unterstellte Person dürfen die Attribute ausschliesslich im Rahmen des Föderationsvertrages bearbeiten, es sei denn, dass sie gesetzlich zur Bearbeitung verpflichtet sind.

<sup>3</sup>Als Dritte im Sinne von Absatz 1 sind Auftragsbearbeiter zu verstehen, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Die Geschäftsstelle ist zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen verpflichtet, angemessene und gesetzeskonforme vertragliche Vereinbarungen abzuschliessen sowie angemessene und zumutbare Kontrollmassnahmen zu ergreifen. Der Einsatz von Dritten oder Wechsel der bestehenden Dritten ist zulässig, soweit

- a. die Geschäftsstelle eine solche Auslagerung der Steuergruppe eine angemessene Zeit vorab schriftlich anzeigt,
- b. die Steuergruppe nicht innerhalb von 30 Tagen ab Mitteilung gegenüber der Geschäftsstelle schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt,
- c. der konkrete Drittanbieter in einem von der Geschäftsstelle erarbeiteten Zusatz zum massgebenden Föderationsvertrag mit dem Identitätsanbieter als genehmigt aufgelistet wird und

- d. die entsprechenden Auftragsbearbeitungsverträge insbesondere die gesetzlichen Anforderungen an Datenschutz und Datensicherheit sicherstellen.

<sup>4</sup>Die Verlagerung der Datenbearbeitung in ein Land, das nicht Mitglied der Europäischen Union oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ist oder über kein nach Schweizer Recht angemessenes Datenschutzniveau verfügt, ist unzulässig.

#### *Art. 12 Datenkategorien*

<sup>1</sup>Die Geschäftsstelle bearbeitet folgende Attribute:

- a. Vorname
- b. Name
- c. Geburtsdatum
- d. Sprache
- e. Rolle
- f. E-Mail-Adresse
- g. Institution
- h. Bildungsstufe
- i. Zyklus
- j. Kanton
- k. Funktion
- l. Technischer Identifikator
- m. Identitätsanbieter-Identifikation

<sup>2</sup>Zusätzlich zur Bearbeitung der Attribute gemäss Absatz 1 wird die AHVN13 kurzfristig jeweils für die Verknüpfung und die Entkoppelung des technischen Identifikators gemäss Absatz 1 litera l mit der Identitätsanbieter-Identifikation gemäss Absatz 1 litera m bearbeitet. Die AHVN13 ist bei der Verknüpfung beziehungsweise der Entkoppelung nicht sichtbar.

#### *Art. 13 Datenbekanntgabe*

Die Identitätsanbieter gestatten die Freigabe bestimmter Attribute, von denen jeder Dienstleistungsanbieter keine, einige oder alle anfordern kann. Die Geschäftsstelle stellt die Übertragung von Attributen gemäss den Vereinbarungen zwischen Identitäts- und Dienstleistungsanbietern sicher.

#### *Art. 14 Datenaufbewahrung und -löschung*

<sup>1</sup>Die in Artikel 12 aufgeführten Attribute werden von der Geschäftsstelle nicht aufbewahrt. Sie bearbeitet Attribute nur so lange, wie dies im Rahmen der jeweiligen Austauschtransaktion erforderlich ist. Die Attribute werden nach Beendigung jeder Austauschtransaktion gelöscht.

<sup>2</sup>Auf Antrag der betroffenen Person wird die Übertragung von Attributen vermerkt und in Form von Metadaten aufbewahrt.

<sup>3</sup>Metadaten werden auf Antrag der betroffenen Person oder spätestens sechs Monate nach Aufhebung der Verknüpfung des technischen Identifikators und der Identitätsanbieter-Identifikation gelöscht.

#### *Art. 15 Technische und organisatorische Massnahmen*

<sup>1</sup>Die Geschäftsstelle ergreift die erforderlichen technischen und organisatorischen Massnahmen, um den Schutz der Attribute und Metadaten sowie die Sicherheit der Bearbeitung zu gewährleisten. Sie beachtet die Grundsätze ordnungsgemässer Datenbearbeitung und gewährleistet die gesetzlich vorgeschriebenen Datensicherheitsmassnahmen. Die Geschäftsstelle erhebt in regelmässigen Abständen die Informationssicherheitsrisiken und überprüft die implementierten technischen und organisatorischen Massnahmen.

<sup>2</sup>Massnahmen gemäss Absatz 1 sind Massnahmen bezüglich Datenschutz und Datensicherheit sowie bezüglich der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Der Stand der Technik, die Implementierungskosten, die Art, der Umfang sowie die Zwecke der Verarbeitung und die unterschiedliche Eintrittswahrscheinlichkeit sowie Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sind zu berücksichtigen. Die Geschäftsstelle setzt insbesondere die folgenden technischen und organisatorischen Massnahmen um:

- a. *Zutrittskontrolle*: unbefugten Personen ist der Zutritt zu den Einrichtungen, in denen Attribute und Metadaten bearbeitet werden, zu verwehren;



- b. *Zugangskontrolle*: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
- c. *Zugriffskontrolle*: der Zugriff der berechtigten Personen ist auf diejenigen Attribute und Metadaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
- d. *Benutzerkontrolle*: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;
- e. *Bekanntgabekontrolle*: Datenempfänger, denen Attribute und Metadaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;
- f. *Transportkontrolle*: bei der Bekanntgabe von Attributen und Metadaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;
- g. *Eingabekontrolle*: in automatisierten Systemen muss nachträglich überprüft werden können, welche Attribute und Metadaten zu welcher Zeit und welcher Person eingegeben wurden;
- h. *Speicherkontrolle*: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Attribute und Metadaten sind zu verhindern;
- i. *Verfügbarkeitskontrolle*: die Verfügbarkeit von gespeicherten Attributen und Metadaten ist sicherzustellen sowie regelmäßig zu prüfen;
- j. *Trennungsgebot*: die Trennung der Attribute und Metadaten pro Organisation (Mandantenfähigkeit) ist sicherzustellen;
- k. *Datenschutz- und Informationssicherheitsmanagement*: die Einhaltung der Datenschutz- und Informationssicherheitsanforderungen ist sicherzustellen.

<sup>3</sup>Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Geschäftsstelle gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und auf Anfrage den Identitätsanbietern schriftlich mitzuteilen.

*Art. 16 Sicherheitsvorfall und Datenschutzverletzung*

Die Geschäftsstelle informiert die Identitäts- und Dienstleistungsanbieter so rasch wie möglich über einen allfälligen Sicherheitsvorfall oder eine allfällige Datenschutzverletzung im Rahmen der Föderation. Sie arbeitet zu deren Behebung mit den betroffenen Identitäts- und/oder Dienstleistungsanbietern zusammen.

**IV Schlussbestimmungen**

*Art. 17 Finanzierung*

<sup>1</sup>Die Kosten für die Geschäftsstelle und den technischen Betrieb der Föderation werden von der EDK mittels Kantonsbeiträgen getragen.

<sup>2</sup>Die Kosten im Zusammenhang mit der Nutzung der Föderation und dem Betrieb der Föderation im Kanton tragen die Kantone.

<sup>3</sup>Für die Überprüfung der Kosten gemäss Absatz 1 setzt die Steuergruppe ein externes Finanzcontrolling ein.

*Art. 18 Fürstentum Liechtenstein*

<sup>1</sup>Das Fürstentum Liechtenstein kann sich nach Massgabe der Bestimmungen des vorliegenden Organisationsreglements an der Föderation beteiligen.

<sup>2</sup>Es schafft im Fürstentum Liechtenstein die für die Nutzung der Föderation notwendigen rechtlichen und organisatorischen Voraussetzungen.

<sup>3</sup>Es beteiligt sich angemessen an den Kosten für die Geschäftsstelle und den technischen Betrieb der Föderation und trägt die Kosten im Zusammenhang mit der Nutzung der Föderation und dem Betrieb der Föderation im Fürstentum.

*Art. 19 Inkrafttreten*

Das Reglement tritt auf den 1. November 2019 in Kraft.

Scuol, 24. Oktober 2019

Im Namen der Schweizerischen Konferenz  
der kantonalen Erziehungsdirektoren

Die Präsidentin:  
Silvia Steiner

Die Generalsekretärin:  
Susanne Hardmeier