educa

Erlachstrasse 21
3012 Bern

+41 31 300 55 00
info@educa.ch

Föderationsvertrag für den Identitätsanbieter

zwischen

Name der Institution

mit Sitz in [vollständige Adresse der Institution], handelnd durch [Titel, Name, Vorname der unterzeichnenden Person, z.B. Leiter:in der Institution, Frau/Herr Name und Vorname, Kanton],
(im Folgenden «*Identitätsanbieter*»)

und

der Geschäftsstelle Edulog

vertreten durch die Fachagentur Educa, Erlachstrasse 21, 3012 Bern, Schweiz, handelnd durch ihren Direktor, Herrn Toni Ritz, und ein Mitglied der Geschäftsleitung, Herrn Reto Schwendimann
(im Folgenden *«Geschäftsstelle»*)

betreffend

Beitritt zur Föderation der Identitätsdienste im Bildungsraum Schweiz (Edulog) der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK)

Der *Identitätsanbieter* und die *Geschäftsstelle* (im Folgenden «die Parteien») vereinbaren das Folgende:

1. Präambel

a. Der *Vertrag* wird auf der Grundlage des *Organisationsreglements* und der *Leistungsvereinbarung* zwischen der *Steuergruppe* und der *Geschäftsstelle* vereinbart, die beide von der Plenarversammlung der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK) genehmigt wurden.

b. Mit diesem *Vertrag* vereinbaren die Parteien den Beitritt des *Identitätsanbieters* zur *Föderation* für Schulen der Primarstufe, Sekundarstufe I, Sekundarstufe II und der beruflichen Grundbildung.

c. Das *Organisationsreglement (*Anhang I), die *Vereinbarung* zur Bearbeitung der Attribute (Anhang II), das Infoblatt: *Genehmigte Subunternehmer* (Anhang III), das *Manual* «Edulog: die Marke» (Anhang IV), das Kontaktformular (Anhang V) sowie die allfälligen anderen mit dem *Identitätsanbieter* vereinbarten und im Vertrag erwähnten Anhänge sind integraler Bestandteil des *Vertrags.*

2. Terminologie

Die Parteien vereinbaren die folgenden Definitionen, deren Begriffe im Text kursiv gedruckt sind:

Attribute: Personendaten der *betroffenen Personen*, die der *Identitätsanbieter* der *Geschäftsstelle* mitgeteilt hat, wie in der *Vereinbarung* festgelegt;

Betroffene Person: Person, deren Personendaten (*Attribute*) bearbeitet werden, damit sie sich identifizieren und auf die autorisierten Dienste der *Dienstleistungsanbieter* zugreifen, um diese zu nutzen;

Dienstleistungsanbieter: Dienstleistungsanbieter, welcher der *Föderation* beigetreten ist, dem die *Attribute* über die *Geschäftsstelle* mitgeteilt wurden, die es den vom *Identitätsanbieter* genehmigten *betroffenen Personen* ermöglichen, sich zu identifizieren und auf die Dienste zuzugreifen, um diese zu nutzen;

Föderation: Föderation der Identitätsdienste im Bildungsraum Schweiz;

Leistungsvereinbarung: Leistungsvereinbarung zwischen der *Steuergruppe* und der *Geschäftsstelle* sowie deren Verlängerungen, die von der Plenarversammlung der EDK genehmigt wurden;

Manual: Manual «Edulog: die Marke» (Anhang IV);

Organisationsreglement: Organisationsreglement der *Föderation* der Identitätsdienste im Bildungsraum Schweiz vom 24. Oktober 2019 (Anhang I);

Steuergruppe: Steuergruppe der *Föderation*, die gemäss dem *Organisationsreglement* ernannt wird;

Subunternehmer: Verpflichtete Dritte, deren Dienstleistungen direkt zur Erbringung der Hauptaufgaben der *Geschäftsstelle* beitragen.

TechID: Durch die *Geschäftsstelle* ausgestellter technischer Identifikator;

UID: Durch den Identitätsanbieter ausgestellte Identifikationsnummer.

Vereinbarung: Vereinbarung über die Bearbeitung der *Attribute* (Anhang II)

Vertrag: vorliegender Föderationsvertrag für den Identitätsanbieter

3. Vertragsbeginn und -ende

a. Der *Vertrag* und seine Anhänge treten am letzten Unterzeichnungsdatum der Parteien in Kraft.

b. Die Mindestdauer des *Vertrags* beträgt 12 Monate ab seinem Inkrafttreten. Nach Ablauf der Mindestdauer verlängert sich der *Vertrag* automatisch auf unbestimmte Zeit. Unter Einhaltung einer sechsmonatigen Kündigungsfrist gegenüber der anderen Partei kann er jeweils per 30. Juni oder 30. Dezember gekündigt werden.

c. Bei einem schwerwiegenden Verstoss gegen die Datenschutzbestimmungen oder die Bestimmungen des *Vertrags* können die Parteien den Vertrag jederzeit ausserordentlich und mit sofortiger Wirkung kündigen.

d. Jede Kündigung, ob ordentlich oder ausserordentlich, muss schriftlich per eingeschriebenem Brief erfolgen.

e. Ungeachtet einer Kündigung des *Vertrags* verpflichten sich die Parteien in jedem Fall, bis zur Beendigung ihrer Vertragsbeziehungen in gutem Einvernehmen zusammenzuarbeiten.

f. Die Kündigung des *Vertrags* führt ohne weitere Massnahmen zur gleichzeitigen Beendigung der *Vereinbarung*.

4. Zweck der Föderation

a. Gemäss *Organisationsreglement* bezweckt die *Föderation* den Zusammenschluss der im schweizerischen Bildungsraum existierenden Identitäts-Management-Systeme für die Schulen der Primarstufe, Sekundarstufe I und Sekundarstufe II einschliesslich berufliche Grundbildung sowie für das Personal der kantonalen Bildungsverwaltung.

b. Die *Föderation* verfolgt insbesondere das Ziel, allen Parteien, die mit der Identifizierung, Authentifizierung und Autorisierung von Nutzenden für den Zugang zu bildungsbezogenen digitalen Diensten zu tun haben, einen kontrollierten, sicheren, transparenten und zuverlässigen Zugang zu vernetzten Umgebungen der Informations- und Kommunikationstechnologie (IKT) zu bieten.

5. Organisation der Föderation

a. Die Verantwortung für die *Föderation* liegt bei der EDK. Sie überträgt die strategischen und operativen Aufgaben gemäss dem *Organisationsreglement* an:
   i. die *Steuergruppe;*
   ii. die *Geschäftsstelle*.

b. Der Betrieb der *Föderation* steht unter der allgemeinen Aufsicht der *Steuergruppe.* Diese stellt eine breite Vertretung des Bildungssystems, inklusive tertiärer Bildung, sicher.

c. Die *Steuergruppe* hat die Aufgabe, die Erbringung der Dienstleistungen über die *Geschäftsstelle* gemäss *Vertrag* sicherzustellen.

d. Die Finanzierung der Dienste der *Geschäftsstelle* durch die Kantone, einschliesslich Support, Beratung und des technischen Betriebs der *Föderation* wird gemäss *Leistungsvereinbarung* nach dem Verteilschlüssel der Kantone aufgeteilt. Allfällige zusätzliche Kosten, die aufgrund von Kantonseigenheiten anfallen, sind durch diese Kantone entsprechend dem Verursacherprinzip zu bezahlen und werden mit diesen vertraglich geregelt.

e. Jeder Kanton ist dafür verantwortlich, dass die gesetzlichen Bestimmungen und die für den Beitritt und die Nutzung der *Föderation* erforderlichen organisatorischen Massnahmen auf seinem Gebiet eingehalten und verabschiedet werden.

f. Der Zweck und die Organisation der *Föderation* ergeben sich im Übrigen aus dem *Organisationsreglement.*

6. Aufgaben und Leistungen der Geschäftsstelle

a. Gemäss *Organisationsreglement* stellt die *Geschäftsstelle* die operative Führung und die Verwaltung der *Föderation* sicher und übernimmt folgende Aufgaben:
   i. die für die *Identitätsanbieter* erforderlichen technischen Dienste zur Gewährleistung der Schnittstellenfunktion bereitstellen;
   ii. den technischen Betrieb der *Föderation* bereitstellen;
   iii. finale Entscheidungen in Bezug auf die Informationssicherheit und den Datenschutz treffen;
   iv. die Kommunikation innerhalb der Föderation sicherstellen.

b. Die *Geschäftsstelle* bearbeitet die *Attribute* für die *Identitätsanbieter* gemäss *Vertrag, Vereinbarung* und *Organisationsreglement*.

7. Beitritt zur Föderation

a. Die von jedem Kanton bestimmten Institutionen der Primarstufe, Sekundarstufe I und Sekundarstufe II einschliesslich beruflicher Grundbildung können der *Föderation* als *Identiätsanbieter* beitreten.

b. Der *Identitätsanbieter* verpflichtet sich, das für ihn geltende Recht und den vorliegenden *Vertrag* einzuhalten.

c. Der Beitritt des *Identitätsanbieters* erfolgt mit Inkrafttreten des *Vertrags* und seiner Anhänge.

8. Identitätsprüfung, Qualität der Attribute und Assurance Levels

a. Der *Identitätsanbieter* stellt sicher, dass jede für die *Föderation* bereitgestellte Identität einer eindeutigen natürlichen *betroffenen Person* entspricht (Eindeutigkeit und Ausschliesslichkeit).

b. Der *Identitätsanbieter* gewährleistet die Vollständigkeit, Genauigkeit, Aufbewahrung und Aktualisierung der mit den Identitäten verbundenen *Attribute*, die er der Geschäftsstelle mitteilt, sowie deren Zuordnung zu den *TechID*, die er von der *Geschäftsstelle* erhält, gemäss den für sie geltenden gesetzlichen und regulatorischen Anforderungen an die Einstiegs-, Mutations- und Ausstiegsprozesse.

c. Auf der Grundlage einer laufenden Beurteilung durch die *Geschäftsstelle* wird dem *Identitätsanbieter* ein Vertrauenslevel zugewiesen, das von den Mindestwerten der Identitäts-, *Attributs*- und Authentifizierungsprüfungen abgeleitet wird:

Stufe	Identitätsprüfung	Attributsprüfung	Authentifizierungsprüfung
	Alle Massnahmen, die erforderlich sind, um eine Identität sofort zu identifizieren und zu registrieren, einschliesslich der Fähigkeit, eine Identität mit einer realen Person zu verknüpfen und zu bestätigen, dass diese Person tatsächlich im Bildungssystem tätig ist.	Mechanismus, um alle deklarierten und obligatorischen Attribute einer Identität vollständig und korrekt zu erfassen und rechtzeitig Korrekturen im Hinblick auf Veränderungen inklusive Austritt der Person aus dem Bildungssystem vorzunehmen.	Art und Weise, wie die Authentifizierung durchgeführt wird, einschliesslich des Schutzes von Berechtigungsnachweisen während der Übertragung und inwieweit eine Person die tatsächliche Kontrolle über ihre Identität hat.
3	Die Identitätsprüfung wird von einer unabhängigen Stelle durchgeführt. Zur Feststellung der Identität müssen ein offizielles Dokument oder mehrere solche vorgelegt werden, z.B. Reisepass. Für die Durchführung einer Identitätsprüfung ist eine physische Präsenz erforderlich, z.B. bei der Einwohnerkontrolle.	Alle in Art. 12 des *Organisationsreglements* erwähnten *Attribute* werden vollständig für alle Identitäten freigegeben. Die *Attribute* werden mindestens einmal jährlich geprüft und Mutationen oder Fehler werden zeitnah, d.h. spätestens innert 7 Tagen aktualisiert bzw. korrigiert. Anpassungen der *Attribute* werden von einer Behörde vorgenommen oder überprüft.	Neben Ein-Faktor- wird auch Multifaktor-Authentifizierung angeboten, z.B. durch Verwendung eines Authentifikators oder SMS-Tokens. Eine Sicherheitsrichtlinie gewährleistet die Qualität der Authentifizierungsfaktoren, z.B. durch die Verwendung sicherer Passwörter. Automatisierte und proaktive Prozesse überwachen verdächtige Anmeldeaktivitäten, z.B. via SIEM.

2	Die Identitätsprüfung darf vor Ort durchgeführt werden, ohne dass diese zwingend von einer unabhängigen Stelle vorgenommen wird, z.B. an der Bildungseinrichtung.	Die *Attribute* gemäss Art. 12 des *Organisationsreglements* sind mehrheitlich für alle Identitäten freigegeben. Darunter sind zwingend Vorname, Nachname, E-Mail-Adresse, Rolle, Institution und Bildungsstufe freizugeben. Die *Attribute* werden mindestens einmal jährlich geprüft und Mutationen oder Fehler werden zeitnah, d.h. spätestens innert 30 Tagen aktualisiert bzw. korrigiert. Anpassungen bei gewissen Attributen, z.B. Funktion, können von der *betroffenen Person* unter Aufsicht einer unabhängigen Stelle geändert werden.	Nur ein Faktor wird für die Authentifizierung verwendet, z.B. Benutzername / Passwort. Die Verwendung von sicheren Passwörtern wird proaktiv empfohlen oder gefördert, z.B. durch Messung der Passwortstärke. Es gibt Massnahmen zur Gewährleistung der Nachvollziehbarkeit der Anmeldeaktivität.
1	Es sind keine behördlichen Kontrollen der Identitätsprüfung vorhanden, z.B. Selbstregistrierung. Es besteht keine zuverlässige Bindung der Identität mit einer eindeutigen physischen Person (z.B. Bestätigung durch E-Mail-Adresse).	Die *Attribute* gemäss Art. 12 des *Organisationsreglements* sind nur teilweise für alle Identitäten freigegeben. Die Attribute unterliegen keiner Validierung und können ganz oder teilweise vom Benutzer selber bereitgestellt werden, z.B. durch Erstellung eines Benutzerprofils. Änderungen werden ohne zeitliche Garantie vorgenommen.	Nur ein Faktor wird für die Authentifizierung verwendet, z.B. Benutzername / Passwort. Der Benutzer darf seine Passwörter ohne Einschränkung frei wählen.

9. Betriebskontinuität und Suspendierungsprozess

a. Der *Identitätsanbieter* gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit seiner Dienste für die *Föderation* sowie die korrekte Implementierung und Konfiguration sämtlicher Schnittstellen zur *Föderation* inklusive deren Betrieb und Wartung. Der *Identitätsanbieter* bezeichnet zur Gewährleistung des störungsfreien Betriebs durch die *Geschäftsstelle* Kontaktpersonen sowie Stellvertretungen. Die Identität der Kontaktpersonen und der Stellvertretungen sowie ihre Kontaktdaten werden im Kontaktformular benannt (Anhang V).

b. Die *Geschäftsstelle* ist berechtigt, bei Vorfällen, die zu einer schweren Bedrohung oder Verletzung der Freiheiten und Rechte der *betroffenen Personen* führen, den Zugang des *Identiätsanbieters* zur *Föderation* notfallmässig vorübergehend zu sperren (Suspendierung). Die *Geschäftsstelle* informiert den *Identitätsanbieter* umgehend. Die *Geschäftsstelle* übernimmt keine weiteren Verpflichtungen gegenüber dem *Identiätsanbieter* oder Dritten.

10. Haftung

a. Im Falle von Vorfällen gemäss Art. 9 des *Vertrags* schliesst die *Geschäftsstelle* jegliche Haftung und Gewährleistung gegenüber dem *Identitätsanbieter* oder gegenüber Dritten für Schäden jeglicher Art aus, mit Ausnahme von Fällen von Vorsatz oder grober Fahrlässigkeit der *Geschäftsstelle.*

b. Die Haftung für die Bearbeitung der *Attribute* ist in der *Vereinbarung* geregelt.

11. Markennutzungsrecht

Die *Geschäftsstelle* ermächtigt den *Identitätsanbieter* als Unterlizenznehmer die Wort-/Bildmarke «Edulog» gemäss den Vorgaben des *Manuals* in einfacher Lizenz zu verwenden (Anhang IV).

12. Schlussbestimmungen

a. Änderungen an diesem *Vertrag* sind nur gültig, wenn sie Gegenstand eines schriftlichen und von beiden Parteien unterzeichneten Zusatzvertrags sind.

b. Bei Widersprüchen zwischen dem *Vertrag* und den Anhängen oder zwischen den Anhängen ist der *Vertrag* massgeblich, sofern nicht in einem Anhang anders angegeben. Bei Widersprüchen zwischen der deutschen und französischen Fassung des *Vertrags* ist die Sprache der vom *Identitätsanbieter* unterzeichneten Fassung massgeblich.

c. Die Nichtigkeit oder Anfechtbarkeit einer oder mehrere Bestimmungen des vorliegenden *Vertrags* heben die Gültigkeit der übrigen Bestimmungen nicht auf, auch nicht die Gültigkeit der Bestimmungen über die Geheimhaltungs- und Aufbewahrungspflicht. Die Parteien bemühen sich in einem solchen Fall, die ungültige oder anfechtbare Bestimmung durch eine andere gültige und durchsetzbare Bestimmung zu ersetzen, die der weggefallenen Bestimmung am nächsten kommt. Gleiches gilt im Fall von Vertragslücken.

d. Die Übertragung des *Vertrags* sowie die Abtretung von Forderungen, die sich daraus ergeben, bedürfen der Zustimmung der anderen Partei.

e. Der *Vertrag* untersteht ausschliesslich Schweizerischem Recht, unter Ausschluss des IPRG, und hat einen ausschliesslichen Gerichtsstand in Bern.

f. Eine Kopie des *Vertrags* und der Anhänge wird jeder Partei auf digitalem Wege ausgehändigt.

educa

Unterschrift des Föderationsvertrags

Für den *Identitätsanbieter* Name der Institution

Ort und Datum	Vorname und Name Leiter:in der Institution

Für die *Geschäftsstelle* Edulog, vertreten durch die Fachagentur Educa

Ort und Datum	Toni Ritz Direktor	Reto Schwendimann Mitglied der Geschäftsleitung

educa

Organisationsreglement der Föderation der Identitätsdienste im Bildungsraum Schweiz

Anhang I zum Föderationsvertrag für den Identitätsanbieter

Das *Organisationsreglement* der *Föderation* der Identiätsdienste im Bildungsraum Schweiz vom 24. Oktober 2019 der Schweizerischen Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren ist auf der Edulog-Website unter folgendem Link abrufbar:

https://www.edulog.ch/de/beitritt/dokumentation

educa

Vereinbarung über die Bearbeitung der Attribute

Anhang II zum Föderationsvertrag für den Identitätsanbieter

DATUM der zweiten Unterschrift des Vertrags

1. Präambel

a. Die *Vereinbarung* über die Bearbeitung der *Attribute* ist integraler Bestandteil des *Vertrags* und präzisiert diesen. Im Übrigen gilt der *Vertrag.*

b. Im Falle eines Widerspruchs zwischen der *Vereinbarung* und dem *Vertrag* in Bezug auf die Bearbeitung der *Attribute* gilt die *Vereinbarung* vorrangig. Vertragliche Verpflichtungen zur Geheimhaltung und Aufbewahrung bleiben davon unberührt.

c. Änderungen der *Vereinbarung* sind nur in Schriftform und von beiden Parteien unterschrieben gültig.

2. Gegenstand der Vereinbarung

a. Die Parteien schliessen die vorliegende *Vereinbarung* ab, um die Rechte und Pflichten der Parteien in Bezug auf die Bearbeitung der *Attribute* im Rahmen der *Föderation* zu konkretisieren.

b. Die *Geschäftsstelle* bearbeitet die *Attribute* für die *Identitätsanbieter* gemäss *Vertrag, Vereinbarung* und *Organisationsreglement*.

3. Zweck der Bearbeitung von Attributen

a. Die Mitglieder der *Föderation* und die *Geschäftsstelle* verpflichten sich, die *Attribute* für die Umsetzung der in Ziff. 4 des *Vertrags* festgelegten Ziele der *Föderation* gemäss dem Grundsatz der Verhältnismässigkeit zu verwenden.

b. In ihrer Rolle als Schnittstelle zwischen den *Identitätsanbietern* und den *Dienstleistungsanbietern* bearbeitet die *Geschäftsstelle* die *Attribute*, um den *betroffenen Personen* einen einfachen und sicheren Zugang zu bildungsbezogenen digitalen Diensten zu ermöglichen.

c. Die Bearbeitung von *Attributen* zu wissenschaftlichen und statistischen Zwecken ist zulässig, sofern die Datensicherheit gewährleistet ist und die *Attribute* anonymisiert werden.

4. Weisungsbefugnis

a. Die *Geschäftsstelle* bearbeitet die *Attribute* ausschliesslich und in Übereinstimmung mit den Zielen und Vorgaben der *Vereinbarung,* des *Vertrags* sowie des *Organisationsreglements*, oder auf ausdrückliche Anweisung des *Identitätsanbieters*, sofern keine anderslautenden gesetzlichen Verpflichtungen gelten, denen die *Geschäftsstelle* unterliegt.

b. Die *Geschäftsstelle* darf *Attribute* nur auf Anweisung des *Identiätsanbieters* ändern, korrigieren, löschen oder die Bearbeitung einschränken. Die Anweisungen des *Identiätsanbieters* müssen dokumentiert und schriftlich, mindestens per E-Mail, mitgeteilt werden. Mündlich erteilte Anweisungen müssen umgehend schriftlich, mindestens per E-Mail, bestätigt werden.

c. Wenn die *Geschäftsstelle* feststellt, dass eine Anweisung gegen gesetzliche Datenschutzvorschriften verstösst, informiert sie den *Identitätsanbieter.* Bis zur Bestätigung oder zu Änderungen der betreffenden Anweisung durch den *Identitätsanbieter* kann die *Geschäftsstelle* die Ausführung der Anweisung aussetzen.

d. Änderungen, die sich auf den Zweck der Bearbeitung beziehen und Änderungen des Ablaufs mit sich bringen, müssen von den Parteien einvernehmlich genehmigt und dokumentiert werden.

5. Kategorien der Bearbeitung von Attributen

a. Die Bearbeitung von *Attributen* betrifft die folgenden Gruppen von *betroffenen Personen:*

   i. Schülerinnen und Schüler der Primarstufe, der Sekundarstufe I und Sekundarstufe II einschliesslich berufliche Grundbildung;
   ii. Lehrpersonen der Primarstufe, der Sekundarstufe I und Sekundarstufe II einschliesslich berufliche Grundbildung;
   iii. Personal der kantonalen Bildungsverwaltungen.

b. Die *Geschäftsstelle* bearbeitet die durch die *Vereinbarung* festgelegten und durch den *Identitätsanbieter* übergebenen *Attribute.* Die Bearbeitung von *Attributen* betrifft die folgenden Datenkategorien:

   i. Vorname;
   ii. Name;
   iii. Geburtsdatum;
   iv. Sprache;
   v. Rolle;
   vi. E-Mail-Adresse;
   vii. Institution;
   viii. Bildungsstufe;
   ix. Zyklus;
   x. Kanton;
   xi. Funktion;

xii. Technischer Identifikator (*TechID)*;
xiii. Identitätsanbieter-Identifikator (*UID*).

c. Zusätzlich zur vorstehenden Bearbeitung der *Attribute* wird die 13-stellige AHV-Nummer kurzfristig nur zur Verknüpfung und Entkoppelung der *TechID* und *UID* verwendet. Die AHV-Nummer ist während des Vorgangs gemäss Art. 12 Abs. 2 des *Organisationsreglements* nicht sichtbar und wird auch nicht gespeichert.

d. Zusätzlich zur Bearbeitung der oben genannten *Attribute* bearbeitet die *Geschäftsstelle* auf der Plattform my.edulog.ch die Pseudonyme, die von den *betroffenen Personen* bei der Registrierung auf dieser Plattform direkt erstellt wurden, um die Dienste der *Föderation* in Anspruch zu nehmen, ihre E-Mail-Adresse sowie die mit ihnen verbundene *TechID.*

e. Die *Geschäftsstelle* verlangt von jedem *Dienstleistungsanbieter,* dass er die Notwendigkeit der Bearbeitung jeder unter Bst. b aufgeführten Datenkategorie begründet. Die *Geschäftsstelle* prüft die Begründungen.

f. Der *Identitätsanbieter* übermittelt der *Geschäftsstelle* rechtzeitig und so schnell wie möglich alle Informationen, die für eine den rechtlichen Anforderungen entsprechende Bearbeitung der *Attribute* durch die *Geschäftsstelle* erforderlich sind. Der *Identitätsanbieter* informiert die *Geschäftsstelle* gesondert und spezifisch über die besonderen Kategorien der zu bearbeitenden *Attribute* und über alle Besonderheiten, die sich im Laufe der Evaluation ergeben.

6. Modalitäten und Vertraulichkeit der Bearbeitung der Attribute

a. Die *Geschäftsstelle* stellt im Rahmen der *Föderation* die Dienstleistungen für den *Identitätsanbieter* gemäss dem Bundesrecht sicher. Der *Identitätsanbieter* garantiert die ordnungsgemässe Anwendung der Gesetze, denen er unterliegt.

b. Die *Geschäftsstelle* bearbeitet die *Attribute*, um die technischen Leistungen gemäss der *Vereinbarung* und dem Bundesgesetz über den Datenschutz zugunsten des *Identitätsanbieters* zu erbringen.

c. Bei der Durchführung ihrer Dienste stellt die *Geschäftsstelle* sicher, dass das eingesetzte Personal zur Vertraulichkeit verpflichtet und mit den geltenden Datenschutzbestimmungen vertraut ist. Die *Geschäftsstelle* und alle ihr zugeordneten Personen verpflichten sich, die *Attribute* gemäss den Anweisungen des *Identitätsanbieters* sowie den Vorschriften der *Vereinbarung,* des *Vertrags* und des *Organisationsreglements* zu bearbeiten, sofern nicht zwingende gesetzliche Verpflichtungen etwas anderes verlangen.

7. Auslagerung

a. Die *Geschäftsstelle* delegiert den technischen Betrieb der *Föderation* gemäss *Vereinbarung* und *Organisationsreglement* an Dritte. Die genehmigten *Subunternehmer* sind im Anhang III des *Vertrags* aufgeführt.

b. Als *Subunternehmer* gelten nur Dritte, deren Dienste direkt zur Erbringung der vertraglichen Hauptleistungen der *Geschäftsstelle* beitragen. Dritte, die von der Geschäftsstelle für Nebenleistungen beigezogen werden, gelten nicht als Subunternehmer (Beispiele für Nebenleistungen: Telekommunikationsdienste, Post- und Transportdienstleistungen oder Reinigungsdienste).

c. Um sicherzustellen, dass die *Subunternehmer* und beauftragten Dritten die gesetzlichen Bestimmungen zum Datenschutz und zur Datensicherheit sowie die vertraglichen Verpflichtungen der *Geschäftsstelle* gegenüber dem *Identitätsanbieter* einhalten, schliesst die *Geschäftsstelle* mit den *Subunternehmern* und beauftragten Dritten vertragliche Ad-hoc-Vereinbarungen ab. Die *Geschäftsstelle* führt angemessene und zumutbare Kontrollmassnahmen ein.

d. Der Einsatz oder der Wechsel von *Subunternehmern* wird gemäss *Organisationsreglement* von der *Steuergruppe* genehmigt. Nach der Genehmigung informiert die *Geschäftsstelle* den *Identitätsanbieter* mindestens 30 Tage im Voraus schriftlich über die geplante Auslagerung. Die Parteien vereinbaren diese Änderungen durch einen Nachtrag zu Anhang III des *Vertrags.* Falls der *Identitätsanbieter* innerhalb von 15 Tagen, nachdem der *Identitätsanbieter* die Information über die Auslagerung erhalten hat, Einspruch erhebt, versuchen die Parteien, eine Einigung zu finden. In dieser Zeit kann die *Geschäftsstelle* ihre Dienste gegenüber dem *Identitätsanbieter* einstellen. Kommt es innerhalb von 60 Tagen nach Eingang des Einspruchs bei der *Geschäftsstelle* zu keiner Einigung, können die Partien den *Vertrag* kündigen.

8. Kommunikation und Ort der Bearbeitung der Attribute

a. Gemäss *Vereinbarung* ermächtigt der *Identitätsanbieter* die *Geschäftsstelle* zur Weitergabe der *Attribute,* die für die Erbringung des gewünschten Dienstes erforderlich sind. Die *Geschäftsstelle* sorgt gemäss den vertraglichen Vereinbarungen für die Übermittlung der *Attribute* an die *Dienstleistungsanbieter.*

b. Damit der *Identitätsanbieter* die Kommunikation der *Attribute* an die verschiedenen *Dienstleistungsanbieter* verwalten kann, stellt die *Geschäftsstelle* dem *Identitätsanbieter* die Funktion der Whitelist der *Dienstleistungsanbieter* zur Verfügung. Diese Funktion ermöglicht es dem *Identitätsanbieter,* den Identifikations-, Authentifizierungs- und Autorisierungsprozess über die *Föderation* bei den einzelnen *Dienstleistungsanbietern* jederzeit zuzulassen oder zu blockieren.

c. Falls der *Identitätsanbieter* die Whitelist nicht verwendet, werden bei der Identifikation, Authentifizierung und Autorisierung einer *betroffenen Person* über die Föderation die erforderlichen *Attribute* an den jeweiligen *Dienstleistungsanbieter* übermittelt, damit dieser die Zugangsrechte der *betroffenen Person* zu den erforderlichen Diensten und deren Nutzung überprüfen kann.

d. Um von dieser Whitelist profitieren zu können, muss der *Identitätsanbieter* diese bei der *Geschäftsstelle* beantragen.

e. Die Weitergabe von Informationen und Auskünften an Dritte oder an *betroffene Personen* durch die *Geschäftsstelle* bedarf der vorherigen schriftlichen Zusage des *Identitätsanbieters.*

f. Die Weitergabe und Bearbeitung von *Attributen* ins Ausland ist unter der Voraussetzung zulässig, dass der Empfängerstaat gemäss Bundesgesetz über den Datenschutz als ein Land gilt, das im Vergleich zum Schweizerischen Recht ein angemessenes Schutzniveau gewährleistet.

g. Die Weitergabe an einen ausländischen Staat sowie die Bearbeitung von *Attributen* durch einen ausländischen Staat, der die Bedingungen von Bst. f nicht erfüllt, bedarf der Zustimmung des *Identitätsanbieters* und der Erfüllung der Bedingungen des Bundesgesetzes über den Datenschutz.

9. Sicherheit der Attribute

a. Um die Sicherheit der Bearbeitung der *Attribute* im Rahmen der Vereinbarung zu gewährleisten, vereinbaren die Parteien konkrete technische und organisatorische Massnahmen.

b. Die *Geschäftsstelle* ergreift die erforderlichen technischen und organisatorischen Massnahmen, um den Schutz der *Attribute* und Metadaten sowie die Sicherheit der Bearbeitung zu gewährleisten. Sie erhebt in regelmässigen Abständen die Informationssicherheitsrisiken und überprüft die implementierten technischen und organisatorischen Massnahmen. Die *Geschäftsstelle* kann auf angemessene alternative Massnahmen zurückgreifen, wobei sie darauf achtet, dass das Sicherheitsniveau der vorgeschriebenen Massnahmen gewährleistet ist. Auf Anfrage dokumentiert die *Geschäftsstelle* wichtige Änderungen und teilt sie dem *Identitätsanbieter* schriftlich mit.

c. Durch diese technischen und organisatorischen Massnahmen stellt die *Geschäftsstelle* auch sicher, dass geeignete Kontrollen implementiert und regelmässig durchgeführt werden, die den erhaltenen Zertifizierungen entsprechen (zum Beispiel: ISO 27001, ISO 29100 und ISO 29134 oder vergleichbare, zum Beispiel NIST 800-53).

d. Diese Kontrollen beziehen sich auf die Dienste der *Geschäftsstelle* sowie auf den technischen Betrieb, einschliesslich der Politik der Datensicherheit, der Sicherheit des Personals, der materiellen Sicherheit der Räume, der technischen Sicherheit der Lösung und des Betriebs (Zugang, Kryptografie und Kommunikationsnetzwerke) sowie auf deren Prozesse, d.h. die Verwaltung der Vermögenswerte, die Beschaffung und Entwicklung sowie die Verwaltung der Dienste und die Kontinuität des Betriebs.

10. Sicherheitsvorfall und Verletzung der Sicherheit der Attribute

a. Die *Geschäftsstelle* informiert den *Identitätsanbieter* so rasch wie möglich über einen allfälligen Sicherheitsvorfall oder eine allfällige Verletzung der Sicherheit der *Attribute* im Rahmen der *Föderation*. Der *Identitätsanbieter* verpflichtet sich in gleicher Weise gegenüber der *Geschäftsstelle.*

b. Zur Behebung arbeiten die *Geschäftsstelle* und der *Identitätsanbieter* mit der Unterstützung des *Dienstleistungsanbieters* zusammen.

11. Aufbewahrung und Löschung der Attribute

a. Die in Ziff. 5.b. der *Vereinbarung* festgelegten *Attribute* werden von der *Geschäftsstelle* für die zur betreffenden Übermittlung erforderlichen Dauer bearbeitet. Die *Attribute* werden nicht aufbewahrt und am Ende jeder Übermittlung gelöscht.

b. Lediglich eine irreversibel verschlüsselte Version der 13-stelligen AHV-Nummer wird aufbewahrt.

c. Das Pseudonym, die E-Mail-Adresse, die *UID* und die *TechID,* die von der *Geschäftsstelle* auf der Plattform my.edulog.ch bearbeitet werden, sowie die verschlüsselte 13-stellige AHV-Nummer werden so lange aufbewahrt, wie die *betroffene Person* berechtigt ist, auf die Dienste der *Föderation* zuzugreifen.

d. Die *Geschäftsstelle* darf keine Kopien anfertigen, ohne den *Identitätsanbieter* schriftlich zu informieren. Ausgenommen sind Sicherheitskopien, sofern diese zur Erfüllung vertraglicher oder gesetzlicher Verpflichtungen in Zusammenhang mit der Bearbeitung der *Attribute* erforderlich sind.

e. Auf Antrag der *betroffenen Person* wird die Übertragung von *Attributen* vermerkt und in Form von Metadaten aufbewahrt. Metadaten werden auf Antrag der *betroffenen Person* oder spätestens sechs Monate nach der Aufhebung der Verknüpfung der *TechID* und der *UID* gelöscht.

12. Andere Verpflichtungen der Geschäftsstelle

a. Wenn eine *betroffene Person* ein Datenschutzrecht direkt bei der *Geschäftsstelle* geltend macht, leitet die *Geschäftsstelle* den Antrag sofort an den *Identitätsanbieter* weiter.

b. Die *Geschäftsstelle* unterstützt den *Identitätsanbieter* im Rahmen des Möglichen durch angemessene technische und organisatorische Massnahmen bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen infolge eines von einer *betroffenen Person* geltend gemachten Rechts.

c. Wenn die *Geschäftsstelle* gesetzlich verpflichtet ist, eine:n Datenschutzbeauftragte:n zu bestellen, teilt die *Geschäftsstelle* dem *Identitätsanbieter* die Kontaktdaten der, des zuständigen Datenschutzbeauftragten mit.

d. Die *Geschäftsstelle* unterstützt den *Identitätsanbieter* im Rahmen des Möglichen und mit angemessenen Bemühungen bei der Erfüllung seiner Verpflichtungen in Bezug auf die Sicherheit der Bearbeitung der *Attribute*, Meldungen bei der Verletzung der Bearbeitung von *Attributen*, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

e. Die *Geschäftsstelle* informiert den *Identitätsanbieter* umgehend über alle Beschwerden, Anträge, Fragen, Kontrollen und Massnahmen der Aufsichtsbehörde für den Datenschutz, die sich auf die Ausführung der *Vereinbarung* beziehen.

13. Kontrolle durch den Identitätsanbieter

a. Auf Anfrage des *Identitätsanbieters* stellt die *Geschäftsstelle* diesem innerhalb einer angemessenen Frist schriftlich (per Post) alle Informationen und Dokumente zur Verfügung, die für eine Kontrolle durch den *Identitätsanbieter* erforderlich sind.

b. Vor Aufnahme der Bearbeitung der *Attribute* und danach regelmässig vergewissert sich der *Identitätsanbieter* über die technischen und organisatorischen Massnahmen der *Geschäftsstelle.* Zu diesem Zweck kann der *Identitätsanbieter*

   i. Auskünfte bei der Geschäftsstelle einholen;
   ii. sich gegebenenfalls eine Bestätigung eines Sachverständigen vorlegen lassen. Dies kann die Vorlage von Berichten oder Auszügen aus Berichten unabhängiger Instanzen (zum Beispiel: Wirtschaftsprüfer, Revisionsstellen, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit sein;
   iii. sich nach Terminvereinbarung zu den üblichen Geschäftszeiten durch Inspektion vor Ort von der Einhaltung der Vorschriften über Datenschutz und Datensicherheit überzeugen.

14. Verantwortlichkeit und Haftung

a. Der *Identitätsanbieter* ist für die Bearbeitung der Daten der *Attribute* verantwortlich, insbesondere für die Einhaltung der für ihn geltenden Datenschutzbestimmungen, insbesondere für die Rechtmässigkeit der Weitergabe der *Attribute* an die *Geschäftsstelle* sowie die Rechtmässigkeit der Bearbeitung der *Attribute*.

b. Der *Identitätsanbieter* haftet für den möglichen Ersatz von Schäden einer *betroffenen Person* aufgrund einer unzulässigen oder nicht vertragsgemässen Bearbeitung ihrer *Attribute*. Die *Geschäftsstelle* unterstützt im Rahmen des Möglichen und durch angemessene Bemühungen den *Identitätsanbieter* bei der Abwehr von durch *betroffene Personen* geltend gemachten Ansprüchen oder bei aufsichtsbehördlichen Massnahmen.

c. Sofern die Haftung des *Identitätsanbieters* festgestellt wird und er gezwungen ist, der *betroffenen Person* den Schaden zu ersetzen, behält sich der *Identitätsanbieter* vor, einen Regressanspruch gegen die *Geschäftsstelle* geltend zu machen, sofern die *Geschäftsstelle* schuldhaft gegen die vertraglichen Verpflichtungen der Vereinbarung oder gegen die Datenschutzbestimmungen im Sinne des Bundesgesetzes über den Datenschutz verstossen hat oder schuldhaft gegenüber ausdrücklichen Anweisungen des *Identitätsanbieters* gehandelt hat.

15. Beendigung der Vereinbarung

a. Bei Beendigung des Vertragsverhältnisses und nach Erfüllung ihrer Dienste löscht die *Geschäftsstelle* die Daten des *Identitätsanbieters* oder übergibt sie dem *Identitätsanbieter*, je nach Anweisungen des *Identitätsanbieters*, sofern diese nicht im Widerspruch mit einer gesetzlichen Verpflichtung oder einem ausdrücklichen Wunsch der *betroffenen Person* nach Aufbewahrung stehen.

b. Auf Anfrage bestätigt die *Geschäftsstelle* dem *Identiätsanbieter,* dass alle Datenträger sowie alle anderen anvertrauten Dokumente sicher zurückgegeben, vernichtet oder gelöscht wurden und dass keine Daten des *Identitätsanbieters* aufbewahrt werden.

c. Die Verpflichtungen zur Geheimhaltung und zum Datenschutz bestehen auch nach Beendigung des Vertragsverhältnisses fort, solange eine gesetzliche Verpflichtung oder ein schutzwürdiges Interesse besteht. Gesetzliche Auskunftspflichten bleiben vorbehalten.

educa

Infoblatt: Genehmigte Subunternehmer

Anhang III zum Föderationsvertrag für den Identitätsanbieter

DATUM der zweiten Unterschrift des Vertrags

Genehmigter *Subunternehmer* gemäss *Organisationsreglement* (Anhang I des Vertrags).

Unternehmen	ELCA Informatik AG
Strasse und Nummer	Av. de la Harpe 22-24
Adresszusatz	Postfach 519
PLZ/Ort	1001 Lausanne
Land	Schweiz

Änderungen der *Subunternehmer* sind nur unter den Voraussetzungen in Ziff. 7 der *Vereinbarung* über die Bearbeitung der *Attribute*, Anhang II zum Föderationsvertrag für den *Identitätsanbieter* möglich.

educa

Manual «Edulog: die Marke»

Anhang IV zum Föderationsvertrag für den Identitätsanbieter

DATUM der zweiten Unterschrift des Vertrags

Das *Manual* «Edulog: die Marke» mit den darin enthaltenen Anweisungen zur Verwendung der Marke bildet einen integralen Bestandteil des Föderationsvertrags für den *Identitätsanbieter.*

Nur die letzte Version des *Manuals* ist verbindlich. Diese ist auf der Website unter folgendem Link abrufbar: https://www.edulog.ch/de/beitritt/dokumentation

Die *Geschäftsstelle* informiert den *Identitätsanbieter,* wenn das *Manual* aktualisiert wird.

educa

Kontaktformular Identitätsanbieter

Anhang V zum Föderationsvertrag für den Identitätsanbieter

DATUM der zweiten Unterschrift des Vertrags

Der *Identitätsanbieter* informiert die *Geschäftsstelle* über Kontaktpersonen und deren Stellvertretungen und informiert jene Personen direkt in Bezug auf ihre Rolle gegenüber der *Geschäftsstelle*.

Der *Identitätsanbieter* ist verpflichtet, die *Geschäftsstelle* unverzüglich zu informieren, wenn sich die Kontaktpersonen oder die Kontaktdaten ändern.

Kontaktperson Technik

Vorname

Name

Firma/Institution

Adresse

E-Mail-Adresse

Telefonnummer

Stellvertretung Kontaktperson Technik

Vorname

Name

Firma/Institution

Adresse

E-Mail-Adresse

Telefonnummer

educa

Kontaktperson Leitung

Vorname

Name

Firma/Institution

Adresse

E-Mail-Adresse

Telefonnummer

Stellvertretung Kontaktperson Leitung

Vorname

Name

Firma/Institution

Adresse

E-Mail-Adresse

Telefonnummer