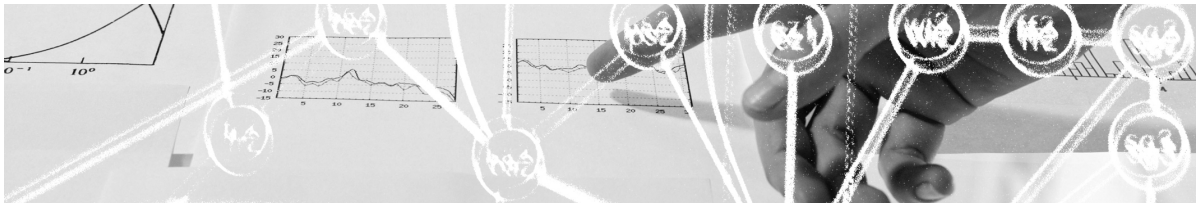
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

# SWITCH edu-ID

## FAQ zum Datenschutz



**Floriane Zollinger-Löw**
**Petra Kauer-Ott**

| | |
|---|---|
| **Dokument-Typ:** | Dokumentation |
| **Version:** | V1.0 |
| **Erstellt am:** | 15.06.18 |
| **Letzte Änderung:** | 06.11.18 |
| **Klassifizierung:** | Public |

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

**Inhalt**



# 1 Was ist SWITCH edu-ID?

Bei SWITCH edu-ID handelt es sich

a) um eine **benutzerzentrierte, langlebige digitale Identität für den Schweizer Bildungs- und Forschungsbereich**. In ihrem Ansatz ähnelt sie der bestehenden SwissID oder anderen sektor-spezifischen digitalen Identitäten wie der europäischen „Open Researcher and Contributor ID“ (ORCID) für Autoren wissenschaftlicher Publikationen;

b) um die **Dienstleistung SWITCH edu-ID**, inklusive benötigter Infrastruktur und Prozesse, welche eine Authentisierung basierend auf einer Basisidentität und spezifischen Attributen[1] innerhalb der AAI Föderation ermöglicht.

[1] Ein Attribut ist eine beschreibende Informationseinheit mit standardisierter Bezeichnung, z.B. Name, E-Mail-Adresse, Geburtsdatum, Telefonnummer, SWITCH edu-ID Identifier etc. Bei den verwendeten Attributen handelt es sich nicht um besonders schützenswerte Personendaten, sondern um sog. Trivialdaten wie Name oder E-Mail-Adresse.

Im Vergleich zur nun seit rund 15 Jahren betriebenen Lösung «SWITCHaai» ermöglicht SWITCH edu-ID eine erweiterte Nutzung von Diensten (z.B. Webdiensten oder mobile Apps) und von Funktionen für alle Organisationen und Dienste, welche zentral bereit gestellt werden können wie z.B. Multi-Faktor-Authentisierung. Als Organisationen gelten z.B. Hochschulen, Bibliotheken, Forschungseinrichtungen oder Spitäler.

SWITCH edu-ID macht die Datenverwaltung für Benutzer transparenter und vereinfacht das Datenmanagement durch die Organisationen. SWITCH edu-ID eröffnet den Zugang zu neuen akademischen Dienstleistungen und für zusätzliche Personengruppen wie Weiterbildungsstudierende, Mitglieder von Forschungsprojekten oder Gäste.

Dieses erweiterte Angebot ist dadurch möglich, dass die Architektur und Funktionsweisen der Dienstleistung gegenüber SWITCHaai verändert wurden, wie die nachfolgende Punkte beispielhaft aufzeigen.

- Die Identität (nachfolgend auch «Konto» genannt) wird vom Benutzer selbst verwaltet (bessere Transparenz und Kontrolle) und bei SWITCH gespeichert.
- Die Identität ist langlebig und damit wiederverwendbar an verschiedenen Organisationen und in unterschiedlichem Kontext. Sie überdauert die Organisationszugehörigkeit(en).
- Eine Identität kann andere und mehr Attribute enthalten als ein AAI-Konto (z.B. mehrere aktive Current Affiliationen[2] oder frühere inaktive Former Affiliations[3]).
- Benutzer können sich wahlweise mit ihrer Basis-Identität als Privatbenutzer anmelden (z.B. bei einer Anmeldung für ein Hochschul-Studium) oder in der Rolle als Mitglied einer Organisation z.B. für den Zugriff auf Lerninhalte.
- Dienste (z.B. das Moodle einer Hochschule oder eine Bibliotheks-Katalog) können bei Bedarf zusätzliche Attribute beziehen (wie Entitlements[4]).
- Bei Änderungen in den Attributen (z.B. Austritt aus einer Organisation oder Änderung eines Namens) wird SWITCH über eine neue Schnittstelle von den Organisationen über die Änderungen informiert. Bei stärkerer edu-ID-Integration kann die Organisation ihrerseits erfahren, wenn Hochschulangehörige Änderungen an ihrer Basis-Identität vornehmen (z.B. Namensänderung) um dann entsprechende Prozesse anzustossen, damit die Änderung/Aktualisierung an der Organisation übernommen werden kann.
- SWITCH übernimmt die Funktion des Identity Providers (Authentisierung) und bietet diese zentral an. Dies bedeutet u.a., dass Attribute bei SWITCH (zwischen-)gespeichert werden.

[2] Eine «Current Affiliation» bezeichnet die aktive Zugehörigkeit zu einer Organisation. Technisch ist sie Teil einer Identität. Eine Current Affiliation beinhaltet mehrere Attribute, welche eine Organisation hinterlegt, um die Authentisierung und Wiedererkennung des Benutzers zu ermöglichen (z.B. E-Mail-Adresse an der Organisation, Name und Rolle).
[3] Eine «Former Affiliation» ist eine Kopie eines Teils einer Current Affiliation und wird bei Ende einer Organisations-Zugehörigkeit von SWITCH erstellt. Sie enthält einen Teil der Daten (Attribute wie Organisation, Rolle (wie Studierender), Study Branch etc.), welche in einer Current Affiliation enthalten waren, plus das Ausstrittsdatum aus der Organisation.
[4] Entitlements sind Attribute welche Informationen zu spezifischen Berechtigungen z.B. in Form einer Gruppenzugehörigkeit enthalten.

Wenn ein Benutzer auf einen Dienst zugreift, werden Attribute mit Einwilligung des Benutzers durch SWITCH an den Dienst weitergegeben.

## 2 Ist SWITCH edu-ID datenschutzkonform?

Ja, SWITCH edu-ID ist datenschutzkonform. SWITCH berücksichtigt bei der Erbringung der Dienstleistung sowohl

a) das **Schweizer Datenschutzgesetz**
   - die aktuelle Fassung [nachfolgend «DSG»]
   - sowie den Entwurf des revidierten Gesetzes [nachfolgend «E DSG»], als auch

b) die **europäische Datenschutzgrundverordnung** (nachfolgend «DSGVO»).

Da die **kantonalen Datenschutzgesetze** dem Schweizer Datenschutzgesetz sehr ähnlich sind und eine Vereinheitlichung und Anpassung der kantonalen Gesetze an die europäischen Bestimmungen absehbar ist, sind in der Regel auch alle kantonalen Datenschutzbestimmungen eingehalten. Falls eine Organisation trotzdem der Ansicht ist, dass eine bestimmte kantonale oder nationale Bestimmung nicht eingehalten ist, klärt SWITCH die Frage gemeinsam mit der Organisation und prüft prozessuale oder technische Anpassungen.

Betroffene Personen wie Datenschutz- oder Sicherheitsbeauftragte von Organisationen können sich bei Fragen direkt an legalteam@switch.ch wenden.

## 3 Welche Rolle spielt die DSGVO?

Da SWITCH keine Niederlassung in der EU hat, grundsätzlich kein Angebot an Kunden in der EU richtet und auch nicht das Verhalten von betroffenen Personen in der EU beobachtet, ist die europäische Datenschutzgrundverordnung (DSGVO) auf SWITCH nicht direkt anwendbar. Als Auftragsdatenbearbeiterin der Organisationen darf SWITCH die Daten der Organisationen aber nur so bearbeiten, wie diese dies selbst tun dürften. Da die Organisationen (insbesondere die Schweizer Hochschulen) in der Regel der DSGVO unterstehen, muss sich auch SWITCH an die entsprechenden Bestimmungen der DSGVO halten. Wie in Ziff. b) oben erwähnt, hält SWITCH alle massgeblichen Bestimmungen der DSGVO ein. Alle Antworten in diesem Dokument berücksichtigen nebst dem Schweizer Gesetz auch die massgeblichen Bestimmungen der DSGVO.

SWITCH richtet sich bei der Bearbeitung von Daten auch deshalb nach der europäsichen DSGVO, weil das revidierte Schweizer Datenschutzgesetz (welches direkt auf SWITCH anwendbar sein wird) stark an die DSGVO angepasst wird und SWITCH für alle Datenbearbeitungen innerhalb der Unternehmung einen einheitlichen Standard festsetzen möchte.

# 4 Details zum Datenschutz

## 4.1 Welches sind die Verwendungszwecke von SWITCH edu-ID?

Grundsätzlich können zwei **Verwendungszwecke** von SWITCH edu-ID unterschieden werden:

a) Verwendung im Rahmen der gewöhnlichen **Hochschuladministration**, z.B. im Rahmen der bestehenden Registrierungsprozesse neuer Studierender («Zweck A»)

b) Verwendung **durch Benutzer um auf eigene Initiative auf Inhalte und Leistungen von Diensten zuzugreifen**, die vom und/oder für den akademischen Sektor angeboten werden («Zweck B»).

Je nach Verwendungszweck sind unterschiedliche gesetzliche Grundlagen relevant (vgl. Ausführungen zum Grundsatz der Gesetzmässigkeit unten).

## 4.2 Von wem erhält SWITCH Daten?

Grundsätzlich stammen Daten

- vom Benutzer (Basis-Identität),
- von Organisationen wie Hochschulen, oder
- von dritten Stellen, welche wie Organisationen in der Rolle eines Attribute Providers (verifizierte) Attribute oder Entitlements für einen Benutzer ausgeben können.

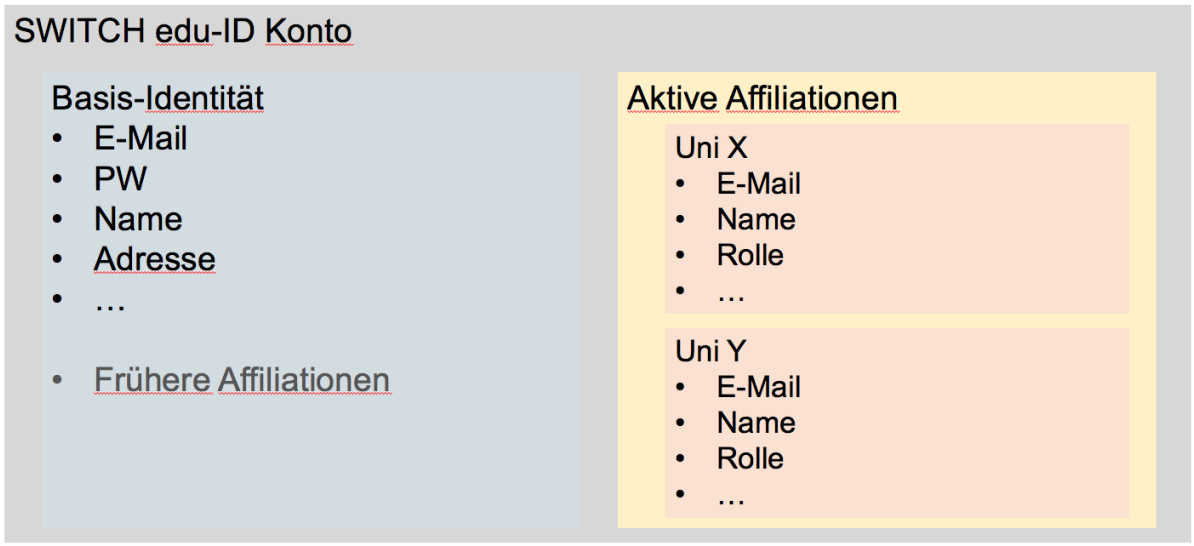
Die hinterlegten Daten können Benutzer

- in «My edu-ID» (d.h. in ihrem Konto auf edu-id.ch) ersehen, und
- im Attribute Viewer (https://attribute-viewer.aai.switch.ch/), welcher primär dem Debugging dient.

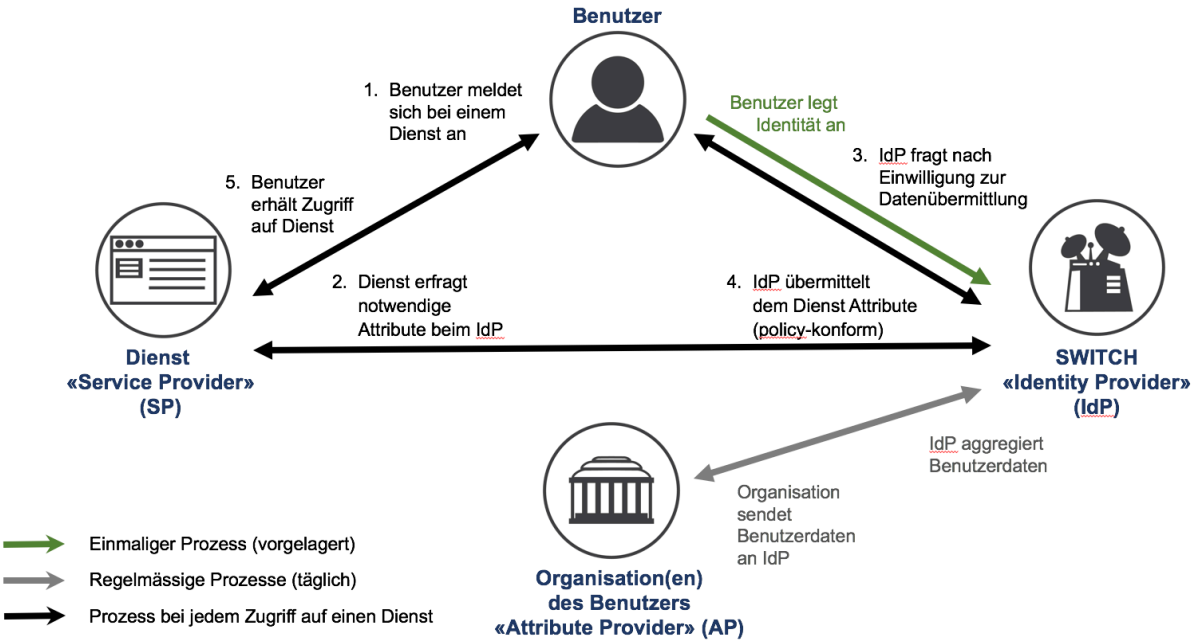
Der Identifikator wird aus Sicherheitsgründen nicht angezeigt.

## 4.3 Welche Daten sind in einem SWITCH edu-ID Konto hinterlegt?

Das Konto eines Benutzers enthält seine Basisidentität und – sofern vorhanden – Affiliationen von Organisationen («Organisations-Identitäten»). Die Daten der aktiven Affiliationen werden von den Organisationen an SWITCH übermittelt. Es können alle Attribute vorhanden sein, welche eine Organisation verwendet oder nur ein Teil davon (abhängig von der Freigabe durch die Organisation). Informationen über frühere Affiliationen werden der Basisidentität hinzugefügt, wenn eine Person aus einer Organisation austritt (vgl. Fussnote 3). Das Qualitätsniveau der einzelnen Attribute ist im Konto ebenfalls ersichtlich.




## 4.4 Wie sehen die Datenflüsse aus?




Die Basis-Identität wird beim Erstellen des Kontos angelegt. Falls es aktive Affiliationen eines Benutzers gibt, werden diese bei SWITCH aggregiert.
Wenn ein Benutzer auf einen Dienst zugreift (1), erfragt der Dienst die benötigten Attribute beim zentralen SWITCH IdP (2). Der IdP fragt in der Folge den Benutzer, ob er der Datenübermittlung an diesen Dienst zustimmt (3). Falls dieser seine Zustimmung erteilt, transferiert der zentrale IdP die erforderlichen Attribute policy-konform an den Dienst (4) und der Benutzer erhält Zugang zum Dienst

(5). Der Benutzer kann einstellen, ob er bei jedem Zugriff auf einen bestimmten Dienst seine Einwilligung geben will, oder erst wieder, wenn Attribute geändert wurden.

## 4.5 Bei welchen Prozessen werden welche Daten bei SWITCH bearbeitet?

Benutzerdaten werden in Form von Attributen gespeichert. Zu einem Attribut gehört jeweils eine Statusangabe, welche die Qualität des Attributs angibt, sowie ein Datum (Erstellung oder Änderung). Die meisten gespeicherten Daten sind im edu-ID Konto des Benutzers zu sehen. Daneben werden History (Änderungen) gespeichert und bestimmte Prozesse und Aktionen geloggt, wenn dies zum Betrieb nötig ist (z.B. Nachvollziehbarkeit von Aktionen, welche zu Fehlern führen; Beweisführung bei Missbrauch).

- Beim **manuellen Erstellen eines Kontos** werden selbst-deklarierte Daten des Benutzers wie Name, Vorname, Adresse, Geburtsdatum, mindestens eine verifizierte E-Mailadresse und ein verschlüsseltes Passwort gespeichert.

- Beim **Erstellen eines edu-ID Kontos auf Basis eines AAI-Kontos** oder beim **Linken mit einem bestehenden AAI-Konto oder einem Konto einer Organsiation** werden die Attribute des betreffenden Kontos von der Organisation in das edu-ID Konto übernommen. Zusätzlich wird der Identifikator hinterlegt, welchen die Organisation verwendet.

- Beim **Verifizieren von Attributen** (nötig für den Zugriff auf bestimmte Dienste; Verifizierung angestossen bei Bedarf) werden verifizierte Attribute wie geprüfte E-Mail-Adressen (welche alle für den Login verwendet werden können), geprüfte Mobilnummer(n) oder eine veifizierte Wohnadresse hinterlegt (weitere Prüfungen können in Zukunft vorgesehen werden). Diese Daten liefert und speichert der Benutzer selbst.

- Beim Linken eines Kontos mit einer **ORCID** hinterlegt der Benutzer bei SWITCH seinen ORCID Identifikator. Dieser wird von https://orcid.org/ herausgegeben.

- Bei **Änderungen** werden geänderte Attribute bei SWITCH hinterlegt. Diese können von jeder authorisierten Stelle stammen, welche Attribute für einen Benutzer innerhalb der Föderation ausstellen kann (Benutzer, spezielle Dienste, Organisationen als Attribute Provider).

- Beim Wegfall einer aktiven Affiliation erstellt SWITCH eine Kopie dieser «Current Affiliation» und hinterlegt sie als «**Former Affiliation**» (frühere Affiliation) mit Enddatum im Konto des Benutzers. Eine Former Affiliation kommt nur im extended attribute model zum Einsatz und wird nur an Dienste ausgegeben (z.B. eine Regstrierungsapplikation einer Alumni-Portal).

- Bei SWITCH ist auch die Information hinterlegt, wann und auf welchem Dienst ein **Login** eines Benutzers stattgefunden hat. Diese Information wird für statistische Zwecke (anonymisiert) pro Dienst und Organsation ausgewertet. Sie dient ausserdem dazu, Probleme, welche durch eine **Duplikatsbereinigung** auftreten können, lösen zu können, indem Dienste, welche ein Benutzer verwendet hat, über die Kontozusammenführung und den neuen Identifikator informiert werden. Damit Benutzer sich von einzelnen Diensten abmelden können, muss SWITCH auch erfassen, bei welchen Diensten ein Benutzer aktuell angemeldet ist (Single Logout).

- Attribute Provider von Organisationen oder bestimmte authorisierte Dienste können **zusätzliche Attribute** (z.B. in Form von Entitlements oder Gruppenzugehörigkeiten) bei SWITCH hinterlegen, um einem Benutzer z.B. Zugang zu Bibliotheksinhalten zu ermöglichen.

- Für den **Support** speichert SWITCH Inhalte von E-Mails, welche normalerweise in Form von Tickets eingehen. Diese Tickets mit Benutzeranfragen werden gespeichert, da Prozess-Logs in edu-ID darauf Bezug nehmen, z.B. wenn eine Identität zusammengeführt oder gelöscht werden soll.

## 4.6 Welche Rollen haben SWITCH, die Organisationen und die Endbenutzer?

Bei **Verwendungszweck A** gilt SWITCH als «**Auftragsdatenbearbeiterin**» der Organisationen. Die Organisationen gelten als «**Verantwortliche**» im Sinne des Gesetzes. Endbenutzer, also betroffene Personen, welche die SWITCH edu-ID benutzen (Studenten, Mitarbeitende etc.) sind sogenannte «**Datensubjekte**».

Bei **Verwendungszweck B** gelten die Organisationen nach Auffassung von SWITCH als **Auftragsdatenbearbeiter der betroffenen Personen** (siehe dazu mehr unter Ziff. 4.8 unten). SWITCH ist **Sub-Auftragsdatenbearbeiterin**.

## 4.7 Welche Pflichten hat SWITCH als Auftragsdatenbearbeiterin?

Als Auftragsdatenbearbeiterin darf SWITCH Personendaten nur so bearbeiten, wie die Organisationen es selbst tun dürften (Art. 10a DSG). Als Auftragsdatenbearbeiterin untersteht SWITCH bspw. allen auf die Organisation anwendbaren **Amtsgeheimnispflichten** und sonstigen Geheimhaltungsverpflichtungen hinsichtlich der bearbeiteten Daten. SWITCH verpflichtet das eigene Personal schriftlich zur Geheimhaltung. Weiter verpflichtet sich SWITCH vertraglich dazu, **Personendaten nur gemäss Weisungen der Organisationen zu bearbeiten**.

Die Organisationen sind zudem vertraglich berechtigt, bei SWITCH die Einhaltung der datenschutzrechtlichen Bestimmungen entweder selber oder durch einen Dritten im Namen und im Auftrag der Organisation **kontrollieren** zu lassen. Des Weiteren kann sich die Aufsichtsbefugnis allfälliger kantonaler Datenschutzbeauftragter auf SWITCH als Auftragsdatenbearbeiterin erstrecken.

SWITCH garantiert auch vertraglich, dass SWITCH nach dem Austritt einer Organisation aus der AAI-Föderation automatisch die aktiven Affiliationen löscht ohne davon eine Kopie zu behalten und auf Wunsch eine solche Löschung bestätigt. Ebenso löscht SWITCH im Einzelfall aktive Affiliationen nach entsprechender Aufforderung der Organisation, ohne dass eine Former Affiliation erstellt wird oder eine Kopie der Affiliation behalten wird. Die Löschung wird auf Wunsch bestätigt.

## 4.8 Welche Pflichten haben die Organisationen als Verantwortliche?

Als Verantwortliche müssen die Organisationen **kontrollieren**, dass bei der Bearbeitung von Personendaten alle **Bearbeitungsgrundsätze und weitere Grundsätze eingehalten** werden. Dies galt bereits für die Dienstleistung SWITCHaai und die AAI-Föderation auf welcher SWITCH edu-ID basiert. Nachfolgend wird aufgezeigt, welches die zu beachtenden Grundsätze sind und **wie SWITCH für deren Einhaltung sorgt**.

- **Grundsatz der Verhältnismässigkeit (z.B. Art. 4 Abs. 2 DSG)**
  Daten dürfen nur verhältnismässig bearbeitet werden. Die europäische Datenschutzgrundverordnung sieht den Grundsatz der **Datensparsamkeit** vor. Dies bedeutet hauptsächlich, dass nur so viele Daten gesammelt werden dürfen, wie für den Betrieb der Dienstleistung nötig ist und dass die Daten nur so lange wie nötig gespeichert werden dürfen. Bei SWITCH edu-ID werden nur diejenigen Attribute bearbeitet, welche für den Betrieb der Dienstleistung nötig sind. So werden nur diejenigen Attribute an Dienste weitergeleitet, welche die Dienste für den Betrieb ihrer Dienstleistung benötigen.

- **Grundsatz der Zweckbindung (z.B. Art. 4 Abs. 3 DSG)**
  Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung **angegeben** wurde, aus den Umständen **ersichtlich** oder **gesetzlich vorgesehen** ist. SWITCH garantiert, dass die Attribute nur für diejenigen Zwecke verwendet werden, die im Dienstleistungsbeschrieb aufgeführt sind. Insbesondere werden keine Daten zu Werbe- oder Marketingzwecken verwendet oder an Dritte weiterverkauft.

- **Grundsatz der Erkennbarkeit (z.B. Art. 4 Abs. 4 DSG), Informationspflicht (z.B. Art. 17 ff. E DSG, Art. 13, 14 DSGVO)**
  Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen **für die betroffene Person erkennbar** sein. SWITCH führt im Dienstleistungsbeschrieb und in den Nutzungsbedingungen transparent und in leicht verständlicher Sprache auf, für welche Zwecke die Daten der Benutzer verwendet werden. Jeder Benutzer muss bei Erstellung eines Kontos die Nutzungsbedingungen akzeptieren. SWITCH übernimmt so für die Hochschulen die Informationspflicht gegenüber den Betroffenen.

- **Grundsatz der Gesetzmässigkeit (z.B. Art. 17 DSG)**
  - Bundesorgane (ETH, EPFL) und kantonale Organisationen brauchen für die Bearbeitung von Personendaten grundsätzlich eine **gesetzliche Grundlage**. Für die Weitergabe von Personendaten an Dritte (z.B. SWITCH) genügt in den meisten Kantonen eine Einwilligung (für weiterführende Informationen zur Datenweitergabe siehe Ziff. 5.1 c im Folgenden).
  - Für die Bearbeitung von Daten zu **Zwecken der Hochschuladministration («Zweck A»)** verfügen die Hochschulen über eine hinreichende gesetzliche Grundlage. Für die Bearbeitung von Daten zu **Zwecken der Benutzer («Zweck B»)** verfügen die Hochschulen zwar nicht über eine entsprechende gesetzliche Grundlage, die **Hochschulen werden aber im Auftrag der Benutzer tätig**, sodass das Erfordernis der gesetzlichen Grundlage entfällt.
  - Vor der Weiterleitung von Daten von den Hochschulen an SWITCH und von SWITCH an die einzelnen Dienste holt SWITCH immer die **Einwilligung der Endbenutzer** ein. Die Einwilligung stellt für die Weiterleitung der Attribute einen hinreichenden Rechtfertigungsgrund dar. Da die Hochschulen nach **Ausscheiden eines Endbenutzers** nicht mehr über eine gesetzliche Grundlage verfügen um dessen Daten bei sich vorhalten zu dürfen, werden Benutzerdaten in Form einer «Former Affiliation» bei Ausscheiden eines Benutzers aus einer Organisation zentral bei SWITCH vorgehalten. Eine solche (inaktive) Affiliation enthält einen Teil der Attribute der früheren Affiliation und kann nach der

Erstellung nicht mehr verändert werden. **SWITCH braucht als privatrechtliche Stiftung für das zentrale Vorhalten der Attribute keine gesetzliche Grundlage.**

- **Richtigkeit der Daten (z.B. Art. 5 DSG)**

  Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. SWITCH prüft in der Basis-Identität hinterlegte E-Mail-Adressen und Mobilnummern auf deren Gültigkeit. Die Qualität von Attributen ist als Information z.B. auch für Dienste verfügbar. Mit unterschiedlichen Methoden der Attributaktualisierung wird sichergestellt, dass die Attribute, welche SWITCH bearbeitet, aktuell sind. Ferner sind die Attribute «Name», «Vorname» und «E-Mail-Adresse» üblicherweise von der Hochschule auf ihre Richtigkeit überprüft worden bevor sie an SWITCH gesendet werden. Mit dem neuen «e-ID-Gesetz» eröffnet sich in Zukunft die Möglichkeit, dass SWITCH von einer qualifizierten Stelle qualifizierte Attribute erhalten könnte, also bspw. einen Namen, der von einer Prüfstelle mittels Ausweiskontrolle überprüft worden ist. Schliesslich überprüft SWITCH bestehende Konten kontinuierlich auf Duplikate hin, was ebenfalls der Richtigkeit der vorhandenen Daten dient. Im User Interface werden den Benutzern Kontaktadressen ihrer Organisation(en) bekanntgegeben, wo sie allenfalls unrichtige oder nicht mehr aktuelle Daten einer Affiliation berichtigen lassen können.

- **Grenzüberschreitende Bekanntgabe (z.B. Art. 6 DSG)**

  - Dienste, auf welche Benutzer mit der edu-ID zugreifen, können sich im Ausland befinden (weltweit). Eine Bekanntgabe von Personendaten in sog. «unsichere Drittstaaten» wie bspw. die USA (vgl. Staatenliste des EDÖB) ist zulässig, wenn im Einzelfall die Einwilligung der betroffenen Person eingeholt wurde oder die Einhaltung eines angemessenen Datenschutzniveaus auf andere Weise sichergestellt wurde. SWITCH als Identity Provider holt mindestens bei der erstmaligen Benutzung eines Dienstes die Einwilligung der Benutzer ein, bevor deren Daten an Diensteanbieter weitergeleitet werden. Der Benutzer kann selber entscheiden, ob er bei jedem Zugriff auf einen Dienst nach seiner Einwilligung gefragt werden möchte oder nur, wenn seine Attribute geändert haben.
  - Die SWITCHaai-Federation Partner können ihre Services von irgend einem Land aus anbieten. Jeder Federation Partner ist über einen Vertrag mit SWITCH ins SWITCH edu-ID legal framework eingebunden.
  - Die SWITCHaai-Federation ist ins Policy Framework des eduGAIN Interfederation Services von GÉANT eingebunden. Dieses Framework regelt die Beziehungen zu Services die über andere Federations weltweit analog eingebunden sind[5].

- **Datensicherheit (z.B. Art. 7 DSG)**
  Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen **unbefugtes Bearbeiten** geschützt werden. SWITCH unternimmt alle zumutbaren Massnahmen, um jederzeit die Datensicherheit gemäss dem jeweils anerkannten Stand der Technik zu gewährleisten. Im Fall von SWITCH edu-ID gehören dazu (vgl. Dienstleistungsbeschrieb):

[5] vgl. SWITCH edu-ID Dienstleistungsbeschrieb https://www.switch.ch/edu-id/terms/.

- Bauliche Massnahmen und Zugangsbeschränkungen zur Server-Infrastruktur
- Zugriffsregelung (Benutzerkonzept, Firewall und dergleichen)
- Regelmässige Serverwartungen
- Automatisierte Dienstüberwachung
- Redundantes Betriebskonzept und Anlegen von Backups zum Schutz vor Datenverlusten
- Datenverschlüsselung und Signatur bei der Übermittlung von Daten
- Förderung einer Kultur der Sparsamkeit bei der Datenweitergabe innerhalb der Föderation
- Einbindung des Endbenutzers in Prozesse welche seine Daten betreffen
- Sensibilisierung des Personals für Datenschutzfragen durch Workshops
- Reglemente und Weisungen
- Verträge

Die Organisation hat das Recht, sich die entsprechenden betrieblichen Prozesse detailliert erklären zu lassen.

- **Wahrung der Betroffenenrechte**
  Die Verantwortlichen (also die Hochschulen) müssen sicherstellen, dass die betroffenen Personen alle ihre Rechte wahrnehmen können. Dazu gehören das **Auskunftsrecht** (Art. 8 DSG, Art. 23 ff. E DSG, Art. 15 DSGVO), das **Berichtigungsrecht** (Art. 5 Abs. 5 E DSG, Art. 16 DSGVO), das **Löschungsrecht** (Art. 5 Abs. 5 E DSG, Art. 17 DSGVO), das **Widerspruchsrecht** (Art. 26 Abs. 2 lit. b E DSG, Art. 21 DSGVO), das Recht auf **Einschränkung der Verarbeitung** (Art. 18 DSGVO) und das Recht auf **Datenportabilität** (Art. 20 DSGVO). SWITCH unterstützt die Hochschulen bei der Sicherstellung dieser Rechte. So beantworten die Organisationen Auskunftsbegehren zwar selber, SWITCH liefert den Hochschulen aber auf erste Aufforderung hin alle erforderlichen Informationen. SWITCH nimmt auf entsprechende Aufforderung hin auch Berichtigungen bei Attributen vor. Weiter hat SWITCH einen Mechanismus implementiert, der auf Wunsch einer betroffenen Person hin das Löschen ihrer Daten ermöglicht (wenn keine aktive Affiliation an einer Organisation besteht). Schliesslich kann SWITCH die Attribute auf Wunsch hin in einem maschinenlesbaren und übertragbaren Format herausgeben. Weiteres zum Löschungsrecht siehe unter Ziff. 4.7 oben und 5.3 a) unten.

# 5 Fragen an die Datenschützer

SWITCH hat seit 2015 mehrere Datenschützer um Rückmeldung zu Architektur und Prozessen von SWITCH edu-ID gebeten, da sich wesentliche Änderungen gegenüber SWITCHaai ergeben. Drei kantonale DatenschützerInnen (Freiburg, Luzern, Zürich) haben zu den Fragen von SWITCH Stellung bezogen. Im Folgenden werden die Fragen von SWITCH, die Antworten der DatenschützerInnen, ergänzende Informationen von SWITCH und jeweils ein Fazit aufgeführt.

## 5.1 Erster Verwendungszweck: Benutzung von SWITCH edu-ID im Rahmen der Hochschuladministration (Zweck A)

a) **Gesetzliche Grundlage**
Beim Verwendungszweck A handelt es sich bei SWITCH edu-ID um ein neues Bearbeitungs*mittel*, das dem bereits anderweitig verfolgten Bearbeitungs*zweck* der Hochschuladministration dient. Mithin ist SWITCH edu-ID denselben Anforderungen von Art. 4 des DSG FR resp. § 5 DSG-LU resp. § 8 Abs. 1 IDG ZH unterworfen wie die allgemeine Bearbeitung von Daten im Rahmen der Hochschulverwaltung.

Teilen Sie die Einschätzung, dass SWITCH edu-ID **durch eine bereits bestehende gesetzliche Grundlage gedeckt** ist, resp. dies gleich wie die bisherige Hochschulverwaltungstätigkeit gerechtfertigt werden kann, wenn die Bestimmungen über die Erfüllung der Aufgaben der Hochschule es voraussetzen?

*Antwort:*
*Ja, da mit der edu-ID heute nur **Trivialdaten** wie Name, Vorname, E-Mail-Adresse und ev. Geburtsdatum erfasst werden und keine Persönlichkeitsprofile entstehen, kann die Bearbeitung der Daten im Rahmen der edu-ID zu Zwecken der Hochschuladministration unter die bestehenden gesetzlichen Grundlagen subsumiert werden und es ist keine zusätzliche gesetzliche Grundlage nötig. Dieser Ansicht sind wie nachstehend aufgeführt auch der DSB ZH und FR. Weshalb der DSB LU für den Einsatz der SWITCH edu-ID generell eine zusätzliche gesetzliche Grundlage verlangt, ist nicht begründet und auch nicht nachvollziehbar.*

Details zu den Antworten der Datenschützer:
Die DSB ZH und FR sind der Ansicht, soweit mit dem neuen Authentifikations- und Authentisierungsprozess Personendaten wie Vorname, Name, E-Mailadresse oder andere, nicht sensitive Personendaten erfasst und bearbeitet würden, könne diese Bearbeitung unter die bestehenden Gesetzesbestimmungen subsumiert werden. Sollten jedoch sensitive oder besonders schützenswerte Personendaten erfasst oder die erhobenen Personendaten mit anderen Merkmalen oder Informationen verknüpft werden, so dass sensitive Informationen oder gar Persönlichkeitsprofile entstehen, sei das Abstützen auf eine formell gesetzliche Grundlage unabdingbar.
Der DSB LU ist der Auffassung, dass der Einsatz der Swiss edu-ID generell einer zusätzlichen gesetzlichen Grundlage bedürfe.

Ergänzende Informationen von SWITCH:
**Besonders schützenswerte Personendaten werden mit der edu-ID heute nicht erfasst** (also bspw. Daten über religiöse, weltanschauliche oder politische Ansichten oder über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse sowie genetische oder biometrische Daten, die eine natürliche Person eindeutig identifizieren).

Sensible Daten oder Profile fallen allenfalls bei den Diensten an (bspw. die Daten eines Bibliothekssystems über das Leseverhalten eines Studenten) oder bei den Hochschulen selber (z.B. die Krankengeschichte von Patienten beim Unispital Zürich). Über diese Daten verfügt SWITCH aber nicht.

Ebenso macht SWITCH **kein «Profiling»** («Profiling» ist die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen, siehe dazu Ziff. 5.4 unten.)

b) **Auftragsdatenbearbeitung**
Ist SWITCH in der Rolle als Dienstbetreiber, welcher im Auftrag der Hochschulen Attribute erhält und weiterleitet, resp. Attribute für die Bedürfnisse der Hochschulen zentral bei sich vorhält als Auftragsdatenbearbeiterin tätig? Welche Anforderungen sind bezüglich der Datenbearbeitungen im Auftrag der Hochschulen durch SWITCH einzuhalten?

*Antwort:*
*Ja, SWITCH ist grundsätzlich als Auftragsdatenbearbeiterin tätig. Entsprechend ist sicherzustellen, dass* ***alle gesetzlichen Vorgaben an eine Auftragsdatenbearbeitung eingehalten*** *sind. SWITCH garantiert, dass alle gesetzlichen Vorgaben an eine Auftragsdatenbearbeitung eingehalten sind. Dazu gehört der Abschluss eines Vertrages mit den Hochschulen (bestehend aus DLB, DLR und Tarif), welcher alle notwendigen Informationen enthält. So garantiert SWITCH in Ziff. 7.2 des DLR u.a. dass Personendaten nur für die vereinbarten Zwecke und gemäss Vorgaben im DLB bearbeitet werden und dass SWITCH allfälligen auf die Organisation anwendbaren Amtsgeheimnispflichten untersteht und das eigene Personal schriftlich zur Geheimhaltung verpflichtet. Weiter verpflichtet sich SWITCH dazu, die Organisationen bei der Einhaltung der auf sie anwendbaren datenschutzrechtlichen Bestimmungen zu unterstützen.*

*Weiter garantiert SWITCH, dass* ***angemessene technische und organisatorische Massnahmen zum Schutz der Daten*** *getroffen werden (siehe Ziff. 7.2 lit. b DLR). Mit dem ausführlichen DLB und den ToU, welche jeder Hochschulverwaltung zugestellt werden und welche zudem von jedem Endbenutzer bei der Registration eines edu-ID-Kontos «abgeklickt» werden müssen, stellt SWITCH zudem sicher, dass die betroffenen Personen und die Hochschulverwaltung* ***vollumfänglich und transparent über die edu-ID und deren aktuelle sowie potentielle Verwendungswecke informiert*** *sind. Gemäss Gesetz wäre es eigentlich die Pflicht des Verantwortlichen (Hochschule) und nicht des Auftragsbearbeiters (SWITCH), die betroffenen Personen über die Verwendung der Daten im Rahmen der edu-ID zu informieren (vgl. Art. 18a DSG, Art. 17 E-DSG). SWITCH nimmt den Hochschulen diese Informationspflicht gegenüber den Betroffenen ab.*

Details zu den Antworten der Datenschützer:
Alle drei Datenschützer halten fest, dass es sich, soweit das Bearbeiten der Attribute im Auftrag der Hochschulen zu Zwecken der Hochschuladministration erfolgt, um ein **«Bearbeiten im Auftrag»** handelt. Die Hochschule ist in diesem Fall «Verantwortliche» und SWITCH eine «Auftragsdatenbearbeiterin». Die **gesetzlichen Vorgaben an eine Auftragsdatenbearbeitung sind einzuhalten**. Dazu gehört der Abschluss eines Vertrages, welcher u.a. das Weisungsrecht der Hochschule und Vertraulichkeitsbestimmungen beinhaltet. SWITCH darf die Daten ferner nur so bearbeiten, wie es die Hochschule selbst tun dürfte. Als Auftragnehmerin ist SWITCH verpflichtet, die für die jeweiligen Hochschulen geltenden gesetzlichen Grundlagen einzuhalten.

*Die DSB ZH hält zudem fest, durch das zentrale Erfassen und Bearbeiten aller gesamtschweizerischen Authentifikations- und Autorisierungsinformationen der Hochschulen in der Schweiz würden aus datenschutzrechtlicher Sicht höhere Risiken für die Betroffenen entstehen, denen mit der Implementierung organisatorischer und technischer Massnahmen Rechnung zu tragen sei. Der DSB LU weist ebenfalls auf das im Vergleich zu SWITCHaai erhöhte datenschutzrechtliche Risiko hin (welches sich insbesondere aus den zusätzlichen Verknüpfungsmöglichkeiten, der höhere Anzahl Attribute sowie der längere Lebensdauer der Attribute ergebe) und merkt an, die Studierenden und die Hochschulverwaltung seien* ***umfassender und transparenter über die edu-ID und deren (potentielle) Verwendungszwecke zu informieren****.*

c) **Anforderungen bezüglich Datenweitergabe**
Welche Anforderungen sind durch die Hochschulen hinsichtlich der jeweiligen Weitergabe von Attributen an SWITCH einzuhalten? Gibt es ausser einer datenschutzkonformen vertraglichen Regelung zwischen SWITCH und der betroffenen Hochschule weitere Voraussetzungen, die geschaffen werden müssen?

*Antwort:*
*Im Fall von* ***Zweck A*** *(Hochschuladministration) ist ein* ***hinreichender Vertrag*** *zwischen SWITCH und den Hochschulen nötig, welcher vorliegt (siehe dazu Ziff. 5.1 b) oben). Im Falle von* ***Zweck B*** *(Zwecke des Benutzers) ist eine* ***Einwilligung der Benutzer*** *nötig. Eine solche holt SWITCH vor jeder Datenbekanntgabe ein. Sobald ein Nutzer auf einen Dienst zugreifen möchte, wird ihm in transparenter und leicht verständlicher Weise aufgezeigt, welche Attribute der Dienst benötigt und die Attribute werden nur übermittelt, wenn der Nutzer der Weiterleitung zustimmt («user consent»).*

Details zu den Antworten der Datenschützer:
Die DSB ZH hält fest, dass unterschieden werden müsse, zu welchen Zwecken Daten von den Hochschulen an SWITCH bekanntgegeben werden. Erfolgt eine Weiterleitung zu **Zwecken der Hochschuladministration (Zweck A)**, so handelt es sich um eine Auftragsdatenbearbeitung, weshalb nur ein Vertrag zwischen SWITCH und den Hochschulen notwendig ist (siehe dazu lit. b oben).

Erfolgt aber eine Weiterleitung zu **anderen Zwecken**, namentlich zum **Zweck B** (Benutzer greift mit der edu-ID auf eine Dienstleistung zu, die von einem Dienst aus dem akademischen Sektor angeboten wird), so ist dies nur unter den Voraussetzungen von §§16 und 17 IDG («Bekanntgabe von Personendaten») möglich, namentlich wenn eine rechtliche Grundlage dazu ermächtigt oder eine **Einwilligung der betroffenen Person im Einzelfall** vorliegt.

Die DSB FR führt als Antwort zu dieser Frage auf, SWITCH dürfe Personendaten nicht zu einem anderen Zweck als zur Hochschuladministration bearbeiten und SWITCH dürfe Daten nicht an Dritte bekanntgeben.

Ergänzende Informationen von SWITCH:
Die Ausführungen der DSB FR, wonach SWITCH die Daten für den Verwendungszweck B nicht verwenden dürfe und wonach eine Weiterleitung an Dritte unzulässig sei, sind nicht nachvollziehbar. Das Gesetz des Kantons Freiburg sieht – wie auch das Gesetz des Kantons

Zürich – ausdrücklich vor, dass eine **Weiterleitung von Daten mit Einwilligung der Nutzer zulässig** ist, und zwar **unabhängig vom Zweck**. Wichtig ist einzig, dass

- die Nutzer transparent über den Verwendungszweck informiert werden,
- sie der Weiterleitung zustimmen und
- die Daten nicht für andere Zwecke verwendet werden, als jene, die dem Benutzer gegenüber mitgeteilt wurden.

Dies wird bei der edu-ID selbstverständlich eingehalten (siehe dazu auch Ausführungen zur Zweckbindung unter Ziff. 4.1 und 4.8 oben).

d) **Erfassung von Attributen durch die Hochschule**
Gibt es bezüglich der ursprünglichen Erfassung der Attribute der Benutzer durch die Hochschule im Vergleich zu den normalen Prozessen der Hochschulverwaltung weitere Voraussetzungen, die eingehalten werden müssen?

*Antwort:*
*Nein, es sind **keine zusätzlichen Voraussetzungen bei der ursprünglichen Erfassung der Attribute durch die Hochschulen zu erfüllen**.*

Details zu den Antworten der Datenschützer:
Die DSB ZH führt aus, dass die Erfassung gestützt auf die **normalen Abläufe im Rahmen der geltenden Rechtsgrundlagen** erfolgt. Wichtig ist insbesondere, dass angemessene Informationssicherheitsmassnahmen umgesetzt werden. Die DSB FR hält fest, die Universität habe sicherzustellen, dass SWITCH die Daten nur so bearbeite, wie die Universität selbst es tun dürfte. Die Universität müsse entsprechende Weisungen erteilen und sich vertraglich absichern. Der DSB LU führt lediglich aus, die Hochschulen hätten im Kanton Luzern die Anforderungen der §§13 und 16 Informatikgesetz (Bestimmungen zur Auslagerung von Informatikdienstleistungen) einzuhalten.

Ergänzende Informationen von SWITCH:
SWITCH teilt die Auffassung der DSB ZH, wonach die ursprüngliche Erfassung der Attribute der Benutzer durch die Hochschulen unter die geltenden rechtlichen Grundlagen subsumiert werden kann. Entsprechend darf davon ausgegangen werden, dass für die ursprüngliche Erfassung von Attributen durch die Hochschulen keine weiteren Voraussetzungen zu beachten sind. Es ist Sache der Hochschulen, sicherzustellen, dass bei der ursprünglichen Erfassung der Attribute angemessene Sicherheitsmassnahmen umgesetzt werden.
Die Aussagen der DSB FR und LU haben mit der gestellten Frage nichts zu tun. SWITCH ist sich bewusst, dass sie die Daten nur so bearbeiten darf, wie die Hochschulen selbst es tun dürften und hält sich daran. Ebenso hält SWITCH alle gesetzlichen Vorgaben im Zusammenhang mit der Auslagerung von Datenbearbeitungen ein (siehe dazu Ziff. 5.1. b) oben).

## 5.2 Zweiter Verwendungszweck: Einsatz von SWITCH edu-ID zu Zwecken des Benutzers (Zweck B)

Die Verwendung von edu-ID zu Zwecken des Benutzers kann einerseits zeitgleich zum ersten Verwendungszweck (Ziff. 5.1 oben) erfolgen. Dies wäre der Fall, wenn ein an der Hochschule eingeschriebener Studierender edu-ID benutzt, um ein Buch eines wissenschaftlichen Verlages online mit

Vergünstigung zu beziehen. Sie kann aber andererseits auch zeitlich verzögert geschehen: Denkbar wäre hier, dass ein Benutzer die Hochschule verlässt, edu-ID aber weiterverwendet, z.B. um seine Studiennachweise und die Unterlagen seines Lebenslaufs zu verwalten.
In diesem Zusammenhang stellen sich folgende Fragen:

a) **Rolle der Hochschule**
Darf davon ausgegangen werden, dass es sich bezüglich der **Rolle der Hochschule im Verhältnis zum Benutzer um eine reine Auftragsdatenbearbeiterin** handelt und das Erfordernis der gesetzlichen Grundlage von Art. 17 Abs. 1 DSG resp. § 8 IDG keine Anwendung findet (da die Hochschule in diesem Fall nicht selbst über den Zweck der Datenbearbeitung entscheidet)?

*Antwort:*
*SWITCH ist wie die DSB ZH und FR der Auffassung, dass die Verwendung von edu-ID zu Zweck B mit **Einwilligung der Nutzer** zulässig ist und **keine zusätzliche gesetzliche Grundlage** nötig ist. Als **Rechtsfertigungsgrund für eine Datenbearbeitung genügt eine gesetzliche Grundlage ODER eine Einwilligung**.*

Details zu den Antworten der Datenschützer:
Die DSB ZH und FR äussern sich beide nicht zur Frage, ob es sich bei der Hochschule in diesem Fall im eine Auftragsdatenbearbeiterin der Benutzer handelt. Sie führen lediglich aus, die Weiterleitung von Attributen an SWITCH zwecks Weiterleitung an die Dienste sei aus Sicht der Hochschulen eine Datenbekanntgabe, welche der Einwilligung der Benutzer im Einzelfall oder einer gesetzlichen Grundlage bedürfe. Die Einwilligung müsse nicht zwingend durch die Hochschulen eingeholt werden, sondern könne auch durch SWITCH eingeholt werden.

Die DSB FR führt zudem aus, die Universitäten hätten keine gesetzliche Grundlage, um eine Einwilligung bei den Studierenden einzuholen. Der DSB LU hält fest, seiner Meinung nach handle es sich bei Zweck B nicht um eine Auftragsdatenbearbeitung durch die Hochschulen, sondern um eine Datenbearbeitung im Rahmen der explizit gesetzlich zu regelnden zusätzlich Aufgaben der Hochschulen. Der DSB LU verlangt also eine neue gesetzliche Grundlage, damit SWITCH edu-ID für den Zweck B verwendet werden darf (er verlangt ausserdem auch eine neue gesetzliche Grundlage, damit die edu-ID für den Zweck A verwendet werden darf, siehe dazu Ziff. 5.1 a) oben).

Ergänzende Informationen von SWITCH:
Die Ausführung der DSB FR, wonach die Universitäten keine gesetzliche Grundlage hätten um eine Einwilligung einzuholen, ist nicht nachvollziehbar. Man braucht keine gesetzliche Grundlage, um eine Einwilligung einzuholen.

Ferner gilt es zu beachten, dass mit der edu-ID im Vergleich zu heute **keine zusätzlichen Daten anfallen oder neue Bearbeitungszwecke** verfolgt werden. Wenn ein Student heute von einem vergünstigten Zeitungs-Abonnement profitieren möchte, und er zu diesem Zweck eine Kopie seiner Legi an einen Verlag schickt, so erfasst dieser die Daten des Studenten auch. Genauso ist es mit den hochschulinternen Diensten: Wenn ein Student heute ein Buch ausleihen möchte, so muss er sich gegenüber dem Bibliotheksdienst ebenfalls legitimieren/ausweisen und seine Daten werden dann vom

Bibliotheksdienst erfasst. Die Hochschulen stellen ihren Angehörigen/Studierenden mit der Legitimationskarte ein Identifikationsmittel zur Verfügung. Dieses wird standardmässig zum Bezug von Diensten der Hochschulen und aus dem akademischen Umfeld (Zweck B) eingesetzt, ohne dass es hierfür eine bestimmte gesetzliche Grundlage gibt. Der Unterschied bei der Verwendung von SWITCH edu-ID zur Legitimierung besteht darin, dass mit edu-ID die Daten des Benutzers einem Bibliotheksdienst oder einem Verlag **elektronisch übermittelt** werden anstelle einer manuellen Erfassung. Bei diesem elektronischen Vorgang werden eher weniger Daten übermittelt als beim «manuellen» Vorgehen, denn die **Datensparsamkeit** ist vertraglich festgelegt und wird durch Organisations- und Dienst-Administratoren geprüft. Nur für den Betrieb erforderliche Daten werden transferiert.

**Anforderungen an die Hochschule als Auftragsdatenbearbeiterin**

b) **Vorkehrungen**
Muss die Hochschule etwas vorkehren, um die Vorhaltung der Daten (zeitgleich zum ersten Verwendungszweck A) zu diesem zweiten Verwendungszweck (B) zu rechtfertigen?

*Antwort:*
*Nein. SWITCH holt vor jeder Datenbekanntgabe die **Einwilligung der Nutzer** ein. Weitere Vorkehrungen müssen nicht getroffen werden.*

Details zu den Antworten der Datenschützer:
Die DSB ZH und FR äussern sich beide nicht zur Frage, ob für die Vorhaltung der Daten bei den Hochschulen zum Zweck B bestimmte Vorkehrungen getroffen werden müssen. Sie führen lediglich aus, vor einer Bekanntgabe der Daten an SWITCH müsse im Einzelfall die Einwilligung der Nutzer eingeholt werden. Der DSB LU verlangt für die Vorhaltung der Daten bei den Universitäten generell eine gesetzliche Grundlage.

Ergänzende Informationen von SWITCH:
SWITCH geht davon aus, dass keine zusätzlichen Vorkehrungen nötig sind, da die Daten einerseits bereits zum ersten Verwendungszweck (A) bei der Hochschule gespeichert werden müssen und es dem Benutzer andererseits freisteht, edu-ID selbst gar nicht zum zweiten Verwendungszweck (B) einzusetzen.

c) **Einwilligung zur weiteren Nutzung beim Austritt**
Reicht es aus datenschutzrechtlicher Sicht aus, wenn der Benutzer vor Austritt aus der Hochschule gefragt wird, ob er SWITCH edu-ID weiterhin nutzen will, um die Übertragung seiner Attribute an SWITCH zu rechtfertigen?

*Antwort:*
*Ja, es reicht aus datenschutzrechtlicher Sicht aus, wenn die Benutzer **vor Austritt aus der Hochschule** gefragt werden, ob sie SWITCH edu-ID weiterhin nutzen wollen. Mit dieser Einwilligung ist die weitere Speicherung der Attribute bei SWITCH datenschutzrechtlich zulässig.*

Details zu den Antworten der Datenschützer:
Alle Datenschützer bejahen diese Frage. Der DSB LU fügt an, die Nutzer müssten vorgängig (vor Austritt) über die Folgen transparent aufgeklärt werden.

d) **Einwilligung zur weiteren Nutzung beim Eintritt**
Ist es zulässig, diese Einwilligung bereits bei der Erstellung eines edu-ID Kontos als Opt-out auszugestalten – dass mit anderen Worten das Konto des Benutzers weitergeführt wird, sofern sich dieser nicht gegenüber SWITCH dahingehend äussert, sein Konto nicht mehr weiterverwenden zu wollen?

*Antwort:*
*Ein **Opt-Out** bezüglich der Weiternutzung von SWITCH edu-ID-Konten nach dem Austritt aus einer Hochschule ist grundsätzlich zulässig.*

Details zu den Antworten der Datenschützer:
Die DSB ZH und FR erachten ein Opt-Out als gangbar, auch wenn sie mit Blick auf die europäische Datenschutzgrundverordnung ein Opt-In bevorzugen würden. Der DSB LU verlangt ein Opt-In. Er begründet seine Antwort damit, dass es sich bei den Konten um Persönlichkeitsprofile resp. besonders schützenswerte Personendaten handle.
Ergänzende Informationen von SWITCH:

Für die Frage, ob das Einholen der Einwilligung als Opt-out ausgestaltet werden kann, kommt es hautpsächlich darauf an, ob man das Schweizer Datenschutzgesetz für Privatpersonen oder die DSGVO als Massstab hinzuzieht. Zudem kommt es darauf an, wie die «Opt-out-Lösung» konktet ausgestaltet wird. Bereits angekreuzte Kästchen etwa, gelten in der Schweiz nach wie vor als eine gültige Einwilligung, wenn das Kästchen Gegenstand einer Erklärung bildet, die ihrerseits einer eindeutigen Willensbekundung der betroffenen Person unterliegt.

e) ***Aufbewahrung und Weiterleitung von Attributen***
Ein SWITCH edu-ID Benutzer kann wie in der bisherigen SWITCHaai-Lösung im Einzelfall über die Weitergabe der benötigten Attribute an den von ihm gewünschten Dienst entscheiden (Anzeige der vom Dienst gewünschten Attribute und Möglichkeit der pauschalen Zustimmung/Ablehnung in Bezug auf alle aufgelisteten Attribute).

Kann diese Kontrollmöglichkeit des Benutzers alternativ zu allfälligen oben aufgeführten Vorkehrungen eine Rechtfertigung bieten für die Aufbewahrung der Attribute durch die Hochschule, die Weiterleitung der Attribute zu SWITCH sowie die Weiterleitung der Attribute durch SWITCH an den Dienst?

*Antwort:*
***Die Einwilligung des Benutzers ist ausreichend** um eine zentrale Speicherung der Daten und eine Datenweitergabe zu Zweck B zu rechtfertigen. Die Hochschulen handeln während eines bestehenden Hochschulverhältnisses als **Auftragsdatenbearbeiter der Benutzer**.*

Details zu den Antworten der Datenschützer:
Die Datenschützer ZH und FR sind sich einig, dass die **Einwilligung genügt** für eine Weiterleitung der Attribute zu SWITCH und für die Weiterleitung der Attribute durch SWITCH an die Dienste. Der DSB LU ist hier anderer Meinung, er verlangt eine gesetzliche Grundlage - jedoch ohne dies zu begründen.
Was die Aufbewahrung von Attributen bei einer Hochschule angeht, so äussert sich die DSB ZH nicht dazu, ob die Einwilligung einen hinreichenden Rechtfertigungsgrund biete, solange das Hochschulverhältnis andauert. Sie führt aber aus, dass die Einwilligung keinen Rechtfertigungsgrund biete für die Aufbewahrung von Attributen durch die Hochschulen nach Beendigung des Hochschulverhältnisses.

Die DSB FR ist der Ansicht, dass die Einwilligung der Benutzer in keinem Fall als Rechtfertigung genüge für die Vorhaltung/Aufbewahrung von Daten durch eine Hochschule (unabhängig davon, ob das Hochschulverhältnis noch besteht oder nicht). Sie verlangt wie der DSB LU eine gesetzliche Grundlage.

Ergänzende Informationen von SWITCH:
Die Hochschulen können nach Beendigung des Hochschulverhältnisses die Attribute mangels gesetzlicher Grundlage nicht mehr bei sich vorhalten. Aus diesem Grund hat sich SWITCH dafür entschieden, die Attribute zentral bei sich vorzuhalten. Als privatrechtliche Stiftung braucht SWITCH keine gesetzliche Grundlage, um Attribute zentral bei sich zu speichern. Notwendig ist einzig die **Einwilligung der Benutzer**, welche SWITCH auch einholt (im DLB, welchen die Benutzer akzeptieren müssen, sind die entsprechenden Bestimmungen aufgeführt).
Was die Vorhaltung/Aufbewahrung von Daten durch die Hochschulen zu Zweck B während laufendem Hochschulverhältnis angeht, so ist SWITCH der Ansicht, dass es sich bei den Hochschulen um Auftragsdatenbearbeiter der Benutzer handelt, und somit keine gesetzliche Grundlage für die Erfassung und Vorhaltung der Daten notwendig ist (siehe dazu auch Ziff. 4.8 oben).

## 5.3 Fragen im Zusammenhang mit der Verwendung von SWITCH edu-ID über einen langen Zeitraum

Während laufendem Verhältnis eines Benutzers zu einer Organisation werden Attribute des Benutzers lokal von der Organisation gespeichert und in Form einer oder mehrerer «Current Affiliationen» an SWITCH übermittelt (siehe Definition von «Current Affiliation» in Fussnoten 2 oben). Eine Kopie dieser aktiven Affiliationen wird zentral bei SWITCH als Betreiberin des Dienstes abgelegt. Nach Austritt des Benutzers aus der Hochschule wird, eine aktive Affiliation in eine «Former Affiliation» umgewandelt. Diese enthält einen Teil der Attribute der früheren «Current Affiliation» und ist zusätzlich mit Enddatum versehen. Sofern der Benutzer sein Konto weiterverwenden möchte, wird diese Information zu einem früheren Organisationsbezug bei SWITCH gespeichert, um v.a. Prozesse, welche mit dem lebenslangen Lernen zusammen hängen, unterstützen zu können.

a) **Löschung eines Kontos**
Muss dem Benutzer eine Möglichkeit gegeben werden, bei SWITCH die Löschung seines Kontos zu verlangen?

*Antwort:*
*Ja. Benutzer können die Löschung ihres Kontos jederzeit verlangen. Solange eine Affiliation mit einer Organisation besteht, darf SWITCH aufgrund des Vertrags mit der Organisation das Konto eines Nutzers jedoch nicht löschen.*

Details zu den Antworten der Datenschützer:
Alle Datenschützer sind sich einig, dass das **Selbstbestimmungsrecht** über die eigenen Daten auch das Recht beinhaltet, die Daten löschen zu lassen.

Ergänzende Informationen von SWITCH:
Alle Benutzer können jederzeit Attribute aus ihrer Basis-Identität selber editieren oder auch löschen – ausser die für den Erhalt des Kontos benötigten Daten. Wenn Benutzer nicht (mehr) bei einer Organisation immatrikuliert/angestellt sind, können sie ihr SWITCH edu-ID Konto jederzeit komplett löschen lassen. Nicht möglich ist jedoch, dass ein Student/Mitarbeiter während laufendem Hochschulverhältnis sein edu-ID Konto löscht, da die Hochschulen SWITCH edu-ID Konten für ihre eigene Hochschuladministration (Zweck A) benötigen. Das Konto ist zwingende Voraussetzung für das Funktionieren von Identitätsmanagementprozessen und für die Benutzerauthentisierung an den Hochschulen.

b) **Anlegen eines neuen «leeren» Kontos**
Ist es zwingend erforderlich, dass der Benutzer die Möglichkeit erhält, ein neues Konto anzulegen, welches keine älteren Attribute aus seinem vorherigen Konto enthält oder ist es zulässig, die Ausstellung eines zweiten Kontos unter Ausschluss früherer Attribute zu verweigern?

*Antwort:*
*Es ist zulässig, die Ausstellung einer zweiten edu-ID unter Ausschluss früherer Attribute zu verweigern, da Benutzer die Möglichkeit erhalten sollen, frühere Affiliationen zu deaktivieren, bzw. deren Weitergabe zu verhindern, wenn sie dies möchten. In begründeten Fällen kann von der Zusammenführung eines älteren Kontos mit einem neuen «leeren» Konto abgesehen werden. Das alte Konto muss dann gelöscht werden.*

Details zu den Antworten der Datenschützer:
Die DSB ZH führt aus, dass die Hochschule über den Prozess der Attributerfassung entscheide. Wichtig sei einzig, dass dieser transparent, also den Nutzenden bekannt sei. Der DSB LU merkt an, seiner Ansicht nach sei dies eine politische Frage. Letztlich sei abzuwägen zwischen dem Recht auf informationelle Selbstbestimmung und dem für einen sinnvollen Einsatz von SWITCH edu-ID erforderlichen Grad an Vollständigkeit der Attribute.

c) **Inaktivierung/Löschung verwaister Konten**
Ist es datenschutzrechtlich erforderlich, Inhaber länger unbenutzter Konten nach Ablauf einer bestimmten Zeit (z.B. nach 5 Jahren) zu kontaktieren und ausfindig zu machen, ob ihre Konten weiterhin zur Verfügung stehen sollen? Ist es zulässig, wenn der Benutzer den Willen der Löschung kundtut oder nicht auf die Kontaktanfrage reagiert, die definitive Löschung seiner Identität nochmals um ein Jahr zu verzögern (z.B. nur Sperrung seiner Daten noch ohne Löschung)?

*Antwort:*
*Es ist zulässig und sinnvoll, dass verwaiste SWITCH edu-ID Konten innerhalb einer Frist von 5-10 Jahren nach letztem Gebrauch deaktiviert und nach einem weiteren Jahr Karenzfrist gelöscht werden.*

Details zu den Antworten der Datenschützer:
Der DSB LU hält diese Regelung für sinnvoll. Die vorgeschlagene Frist von 5 Jahren erscheint ihm verhältnismässig und auch eine abgestufte Lösung mit einer Deaktivierung der Profile in einer ersten Phase und einer Löschung erst in einer zweiten Phase sei möglich und auch sinnvoll. Von den DSB ZH und FR gibt es keine Antworten zu dieser Frage, da ihnen diese damals nicht gestellt wurde.

Ergänzende Informationen von SWITCH:
Es ist SWITCH ist im Hinblick auf das Ziel des lebenslangen Lernens wichtig, die Nutzungsmöglichkeit der Konten auch bei längeren Unterbrüchen sicherzustellen. Eine Karenzfrist soll sicherstellen, dass der Benutzer nachträglich seine Meinung ändern kann, falls er nach einigen Jahren eine universitäre Weiterbildung absolviert oder eine andere Aktivität im Hochschulumfeld aufnimmt.

Eine längere Frist von bis zu 10 Jahren käme den Hochschulen entgegen. Sie könnten ehemalige Benutzer in diesem Fall auch nach längeren Unterbrüchen wiedererkennen.

d) **Aktualisierung der Daten**
d1) Braucht es für die periodisch stattfindende automatische Aktualisierung der Daten («Attribute Aggregator») jeweils eine neue Einwilligung oder darf davon ausgegangen werden, dass eine einmalige Einwilligung genügt?

*Antwort:*
*Eine **einmalige Einwilligung genügt**. Alles andere würde keinen Sinn machen und wäre auch nicht im Interesse der betroffenen Benutzer. SWITCH holt die Einwilligungen der betroffenen Personen ein.*

Details zu den Antworten der Datenschützer:
Hierzu gab es keine Antworten.

d2) Könnte Art. 5 DSG bzw. § 7 Abs. 2 lit. b IDG bzw. als Rechtfertigungsgrund für die periodischen automatischen Aktualisierungen betrachtet werden, wonach Daten richtig und nachgeführt sein müssen, sofern es der Bearbeitungszweck erfordert?

*Antwort:*
*Art. 5 DSG könnte als Rechtfertigungsgrund für die periodischen automatischen Aktualisierungen betrachtet werden.*

Details zu den Antworten der Datenschützer:
Hierzu gab es keine Antworten.

## 5.4 Persönlichkeitsprofile und Profiling

Entstehen durch Sammlung der Attribute Persönlichkeitsprofile i.S.v. Art. 3 lit d. DSG und falls ja, was wären die Konsequenzen?

*Antwort:*

*Es kann nicht ausgeschlossen werden, dass im Rahmen der SWITCHedu-ID Persönlichkeitsprofile bearbeitet werden. Eine Bearbeitung von Persönlichkeitsprofilen ist gemäss Schweizer Datenschutzgesetz mit Einwilligung der betroffenen Person im Einzelfall gerechtfertigt. Die Einwilligungen werden in jedem Einzelfall eingeholt. Das Abstützen auf eine zusätzliche formell gesetzliche Grundlage ist nicht notwendig. Mit Inkrafttreten des revidierten Schweizer Datenschutzgesetzes fällt der Begriff des «Persönlichkeitsprofils» aber ohnehin mit an Sicherheit grenzender Wahrscheinlichkeit weg. Profiling wird im Rahmen der SWITCH edu-ID nicht betrieben.*

Details zu den Antworten der Datenschützer:
Die DSB LU und FR führen aus, falls mit der edu-ID sensitive oder besondere Personendaten erfasst werden sollten oder die erhobenen Personendaten mit anderen Merkmalen oder Informationen verknüpft werden sollten, so dass sensitive Informationen oder gar Persönlichkeitsprofile entstehen, sei das Abstützen auf eine formell gesetzliche Grundlage unabdingbar.
Ergänzende Informationen von SWITCH:

Ein «Persönlichkeitsprofil» ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (Art. 3 lit. d DSG). Von einem Persönlichkeitsprofil ist die Rede bei einer Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch die ausserberuflichen Beziehungen und Tätigkeiten, die ein Gesamtbild oder ein wesentliches Teilbild der betreffenden Person ergeben. Der Begriff des Persönlichkeitsprofils kann nicht generell definiert werden. Für die Frage, ob eine Zusammenstellung mehrerer Daten einer bestimmten Person ein Persönlichkeitsprofil ergibt, sind **Menge** und **Inhalt** der personenbezogenen Informationen massgebend[6].

Der Begriff des «Persönlichkeitsprofils» wird im revidierten Schweizer Datenschutzgesetz in Anpassung an die DSGVO ersetzt durch «**Profiling**». Als «Profiling» gilt die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen (Art. 4 lit. f E-DSG). Die Begriffe «Persönlichkeitsprofil» und «Profiling» weisen zwar Ähnlichkeiten auf, sie sind aber

[6] Beispiele für Persönlichkeitsprofile sind: Die Aufzeichnung von Kartentransaktionen durch ein Kreditkartenunternehmen, mit dem Ziel, festzustellen, ob eine bestimmte Transaktion für einen bestimmten Kunden ungewöhnlich ist; die Aufzeichnung von Einkäufen durch einen Grossverteiler im Rahmen einer Kundenbindungsprogramms mit dem Ziel, sich ein Bild von dem Konsumverhalten der Kunden zu bilden; die Zusammenstellung sämtlicher Daten von Versicherungsnehmern durch eine Versicherung, um besser einschätzen zu können, welche Kunden die interessantesten sind und mit welchen Produkten sie beworben werden sollten.

nicht deckungsgleich. Während das Persönlichkeitsprofil i.d.R. etwas Statisches ist, umschreibt das Profiling einen dynamischen Prozess, welcher zudem auf einen bestimmten Zweck ausgerichtet ist.

Die SWITCH edu-ID besteht aus einer sog. «Basis-Identität», welcher weitere Attribute und Affiliationen hinzugefügt werden können. Alle Attribute (sowohl die Attribute der Basis-Identität als auch weitere hinzugefügte Attribute) werden zentral bei SWITCH gespeichert. Die Attribute in der Basis-Identität sind unter Kontrolle des Benutzers, z.B. Name, Vorname und E-Mail-Adresse. Als weitere Attribute können Benutzer Geburtsdatum, Telefonnummer oder Adresse hinzufügen und Identitäten wie eine ORCID hinterlegen. Weiter verfügt SWITCH über die «Current Affiliation» eines Nutzers, d.h. die Information, ob und falls ja bei welcher Organisation ein Nutzer immatrikuliert/angestellt ist. Zudem verfügt SWITCH über das Attribut «Affiliation», d.h. über die Information, in welcher pauschalen Rolle (Student/Mitarbeiter/Mitglied/Zugehörige Person) ein Nutzer bei einer Organisation erfasst ist. Falls ein Nutzer aus einer Organisation austritt, wird SWITCH von der Organisation über den Austritt informiert und das Attribut-Set «Current Affiliation» wird automatisch umgewandelt in eine «Former Affiliation», d.h. die Information, bei welcher Organisation ein Nutzer bis wann immatrikuliert/angestellt war und ev. weitere Attribute wie Study Branch. Die «Former Affiliation» wird bei SWITCH hinterlegt. Weiter ist es möglich, dass eine Hochschule sog. «Entitlements» an SWITCH übermittelt. Dies sind Attribute, welche Informationen zu spezifischen Berechtigungen enthalten, z.B. in Form einer Gruppenzugehörigkeit (z.B.«Lehrperson» oder «Bibliotheksbenutzer». Diese Attribute werden benötigt, wenn ein Dienst nur Personen zur Verfügung steht, welche einer solchen «Gruppe» Berechtigter angehören. Erfasst wird auch die Sprachpräferenz einer Person. Dies hilft Diensten, das Interface in der vom Benutzer gewünschten Sprache anzuzeigen.

Weiter verfügt SWITCH über die Informationen, welcher Nutzer wann auf welchen Dienst zugegriffen hat (Logdaten). Was SWITCH nicht hat, sind die Informationen, in welcher Art und Weise ein Dienst benutzt wurde. SWITCH weiss also bspw., dass eine bestimmte Person zu einem bestimmten Zeitpunkt auf einen Bibliotheksdienst zugegriffen hat, SWITCH weiss aber nicht, was der Benutzer innerhalb dieses Dienstes gemacht hat oder welches Buch ausgeliehen wurde. Genauso verfügt SWITCH bspw. über die Information, dass eine bestimmte Person zu einem bestimmten Zeitpunkt auf Azure (Microsoft Cloud) zugegriffen hat, SWITCH verfügt aber nicht über die Information, welche Dokumente mit dem Dienst bearbeitet wurden. Diese Informationen fallen nur bei den Diensten an.

**Persönlichkeitsprofil bei grösserer Ansammlung von Daten**

Ein edu-ID-Konto, welches nur aus einer Basis-Identität mit minimalen Attributen (Name, Vorname und E-Mail-Adresse) besteht, gilt kaum als Persönlichkeitsprofil, da es keine Rückschlüsse auf die Persönlichkeit einer Person zulässt. Auch ein physischer Pass oder eine physische Identitätskarte gilt noch nicht als Persönlichkeitsprofil. Je mehr Attribute einem edu-ID-Konto hinzugefügt werden, desto eher liegt aber ein Persönlichkeitsprofil vor. Enthält ein edu-ID-Konto bspw. die über einen längeren Zeitraum angesammelten Informationen, welche Studiengänge eine bestimmte Person in welchem Zeitraum abgeschlossen oder nicht abgeschlossen hat, kann man daraus allenfalls wesentliche Merkmale der Persönlichkeit der Person X abzuleiten versuchen. Es kann nicht ausgeschlossen werden, dass solche Ansammlungen von Attributen über einen längeren Zeitraum hinweg als Persönlichkeitsprofile qualifiziert werden.

**Kein Profiling**

Von einem «Profiling» kann beim Bearbeiten der edu-ID-Daten nicht gesprochen werden und zwar aus folgenden Gründen: Zwar handelt es sich bei der Historie eines Nutzers um eine Datensammlung, welche im Laufe der Zeit angewachsen und somit «dynamisch» ist – die Informationen werden aber nicht zu dem Zweck gesammelt, wesentliche Aspekte der Persönlichkeit der Nutzer zu analysieren oder deren Verhalten vorherzusagen. Der Zweck der Datensammlung liegt einzig und allein in der Verwendung der Daten für die Hochschuladministration oder darin, dass die Nutzer auf Dienste im akademischen Umfeld zugreifen können. Auf keinen Fall wird die Historie der Nutzer analysiert, um diesen bspw. zielgerichtet Werbung für bestimmte Studiengänge schicken zu können. Entsprechend nehmen SWITCH und die Organisationen mit dem Betreiben von SWITCH edu-ID kein «Profiling» an den Nutzern vor.

**Konsequenzen**
Als Konsequenz davon, dass die Zusammenstellung der edu-ID-Daten als Persönlichkeitsprofil qualifiziert werden kann, hat SWITCH **verstärkte Informationspflichten** gegenüber den betroffenen Personen (Art. 14 DSG) und es braucht für die Bearbeitung der Daten die **Einwilligung der betroffenen Personen im Einzelfall** (Art. 17 Abs. 2 lit. c DSG). Weiter muss die **Datensammlung dem EDÖB gemeldet** werden (Art. 11a Abs. 3 lit. a DSG). SWITCH erfüllt alle diese Pflichten.

***