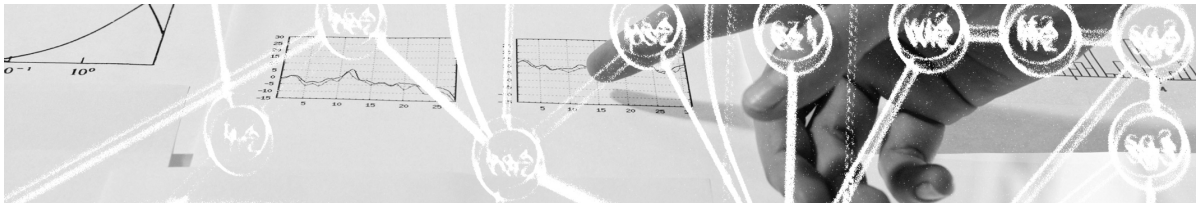
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

SWITCH edu-ID

FAQ sur la protection des données



Floriane Zollinger-Löw
Petra Kauer-Ott

Type de document: Documentation
Version: V1.0
Établi le: mardi, 2 octobre 2018 16:20:00
Dernière modification: jeudi, 8 novembre 2018 14:34:00
Classification: publique

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

Contenu

1 Qu'est-ce que SWITCH edu-ID?

En ce qui concerne SWITCH edu-ID, il s'agit

a) d'une **identité numérique et durable basée sur l'utilisateur pour le domaine de la formation et de la recherche suisse**. Dans son approche, elle se rapproche du SwissID existant ou d'autres identités numériques spécifiques au secteur, comme l'«Open Researcher and Contributor ID» (ORCID) pour les auteurs de publications scientifiques;

b) du **service SWITCH edu-ID**, avec l'infrastructure et les processus requis, qui permet une authentification sur la base d'une identité de base et d'attributs spécifiques[1] au sein de la fédération AAI.

En comparaison avec la solution «SWITCHaai» exploitée depuis désormais 15 ans, SWITCH edu-ID permet une utilisation étendue des services (p. ex. des services web ou des applications mobiles) et des fonctions pour l'ensemble des organisations et services qui peuvent être mis à disposition de

[1] Un attribut est une unité d'information descriptive possédant un nom standardisé, p. ex. nom, e-mail, date de naissance, numéro de téléphone, SWITCH edu-ID Identifier, etc. Les attributs utilisés ne sont pas des données sensibles, mais des données communes comme le nom ou l'adresse e-mail.

manière centralisée, comme p. ex. une authentification multi-facteurs. Sont p. ex. considérés comme des organisations des hautes écoles, des bibliothèques, des institutions de recherche ou des hôpitaux.

SWITCH edu-ID rend la gestion des données transparente pour les utilisateurs et simplifie la gestion des données par les organisations. SWITCH edu-ID ouvre l'accès à de nouvelles prestations de service académiques et à des groupes de personnes supplémentaires comme des étudiants en formation continue, des membres de projets de recherche ou des invités.

Cette offre étendue est rendue possible par le fait que l'architecture et le fonctionnement de la prestation de service sont modifiés par rapport à SWITCHaai, comme le démontrent à titre d'exemple les points suivants.

- L'identité (ci-après désignée «compte») est gérée par l'utilisateur lui-même (meilleure transparence et meilleur contrôle) et enregistrée chez SWITCH.
- L'identité est durable et ainsi réutilisable dans diverses organisations et dans un contexte différent. Elle survit à l'appartenance à une organisation.
- Une identité peut contenir d'autres attributs qu'un simple compte AAI (p. ex. plusieurs affiliations actuelles (current affiliation) actives[2] ou des affiliations anciennes (former affiliations) inactives.[3]).
- Les utilisateurs peuvent s'inscrire au choix avec leur identité de base en tant qu'utilisateur privé (p. ex. pour une inscription à des études dans une haute école) ou avec un rôle de membre d'une organisation, p. ex. pour l'accès à des contenus d'apprentissage.
- Des services (p. ex. le Moodle d'une haute école ou un catalogue de bibliothèque) peuvent récupérer si nécessaire des attributs supplémentaires (comme des entitlements[4]).
- En cas de modifications apportées aux attributs (p. ex. sortie d'une organisation ou changement de nom), SWITCH est informée des changements par les organisations par le biais d'une nouvelle interface. Avec une intégration edu-ID renforcée, l'organisation peut apprendre de son côté si des membres des hautes écoles apportent des modifications à leur identité de base (p. ex. changement de nom), afin qu'elle puisse lancer des processus correspondants dans le but de reprendre la modification/mise à jour au niveau de l'organisation.
- SWITCH assume la fonction d'identity provider (authentification) et propose ceci de manière centralisée. Ceci signifie notamment que les attributs sont stockés (temporairement) chez SWITCH. Si un utilisateur a accès à un service, des attributs relatifs au consentement de l'utilisateur sont transmis par SWITCH au service.

[2] Une «current affiliation» désigne l'appartenance active à une organisation. Techniquement, il s'agit d'une partie d'une identité. Une affiliation active contient plusieurs attributs qu'une organisation enregistre pour permettre l'authentification et la reconnaissance de l'utilisateur (p. ex. l'adresse e-mail dans l'organisation, le nom et le rôle).
[3] Une «former affiliation» est une copie d'une partie d'une affiliation active et est créée à la fin d'une appartenance à une organisation de SWITCH. Elle contient une partie des données (des attributs comme l'organisation, le rôle (p. ex. étudiant), la branche d'études, etc.) qui sont contenues dans une affiliation active, plus la date de sortie de l'organisation.
[4] Des entitlements sont des attributs qui contiennent des informations sur des autorisations spécifiques, p. ex. sous la forme d'une appartenance à un groupe.

2 SWITCH edu-ID est-elle conforme à la protection des données?

Oui, SWITCH edu-ID est conforme à la protection des données. Lors de la fourniture de la prestation de service, SWITCH prend en compte aussi bien

a) la **loi suisse sur la protection des données**
   - dans sa version actuelle [ci-après désignée «LPD»]
   - et le projet de loi révisée [ci-après désignée «P-LPD»] que

b) le **règlement général européen sur la protection des données** (ci-après désigné «RGPD»).

Du fait que les **lois cantonales sur la protection des données** sont très similaires à la loi suisse sur la protection des données et qu'une harmonisation et un ajustement des lois cantonales avec les dispositions européennes sont prévisibles, toutes les dispositions cantonales relatives à la protection des données sont également généralement respectées. Si une organisation est tout de même d'avis qu'une certaine disposition cantonale ou nationale n'est pas respectée, SWITCH étudie la question avec l'organisation et vérifie les ajustements procéduraux ou techniques.

Si elles ont des questions, les personnes concernées comme des responsables de la sécurité ou des délégués à la protection des données d'organisations peuvent s'adresser directement à legalteam@switch.ch.

3 Quel rôle le RGPD joue-t-il?

Vu que SWITCH n'a aucune succursale dans l'UE, qu'elle n'adresse par principe aucune offre à des clients situés dans l'UE et qu'elle ne surveille pas non plus le comportement des personnes concernées dans l'UE, le règlement européen relatif à la protection des données (RGPD) n'est pas directement applicable. En tant que processeur de données dans les organisations, SWITCH peut traiter les données des organisations mais uniquement de la manière dont ces dernières pourraient le faire elles-mêmes. Comme les organisations (notamment les hautes écoles suisses) sont en règle générale soumises au RGPD, SWITCH doit également s'en tenir aux dispositions correspondantes du RGPD. Comme mentionné au point b) ci-dessus, SWITCH respecte toutes les dispositions déterminantes du RGPD. Toutes les réponses données dans ce document prennent en compte les dispositions déterminantes du RGPD, en plus de la loi suisse.

C'est pourquoi SWITCH se base sur le RGPD européen pour le traitement des données parce que la loi suisse sur la protection des données révisée (qui sera directement applicable à SWITCH) est fortement adaptée au RGPD et que SWITCH souhaite définir une norme unifiée applicable à tous les traitements de données au sein de l'entreprise.

4 Informations détaillées relatives à la protection des données

4.1 Quels sont les usages de SWITCH edu-ID?

Par principe, il faut différencier deux **usages** de SWITCH edu-ID:

a) utilisation dans le cadre de l'**administration des hautes écoles** habituelle, p. ex. dans le cadre des processus d'enregistrement existants de nouveaux étudiants («finalité A»)

b) utilisation **par les utilisateurs pour accéder de leur propre initiative aux contenus et prestations de service** qui sont proposés par et/ou pour le secteur universitaire («finalité B»).

En fonction de l'usage, différentes bases légales sont applicables (cf. propos ci-dessous relatif au principe de la légalité).

4.2 De qui SWITCH obtient-elle des données?

Sur le principe, les données proviennent

- de l'utilisateur (identité de base),
- d'organisations telles que des hautes écoles, ou
- d'organismes tiers qui, dans leur rôle d'attribute providers, peuvent émettre des attributs (vérifiés) ou des entitlements pour un utilisateur.

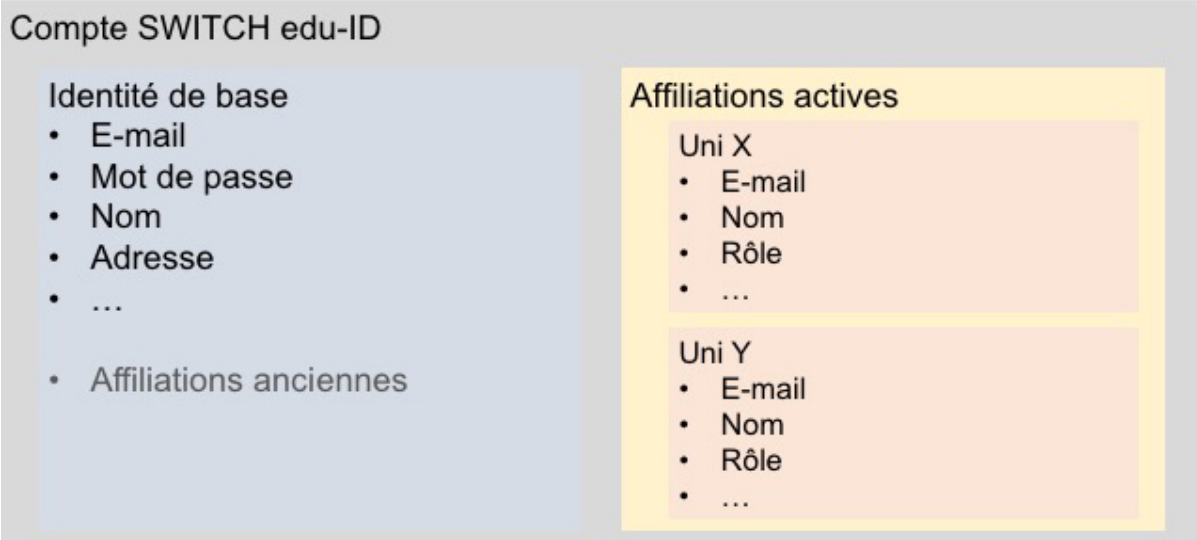
Les utilisateurs peuvent consulter les données stockées

- dans «My edu-ID» (c'est-à-dire dans leur compte sur edu-id.ch) et
- dans l'Attribute Viewer (https://attribute-viewer.aai.switch.ch/) qui sert principalement au débugage.

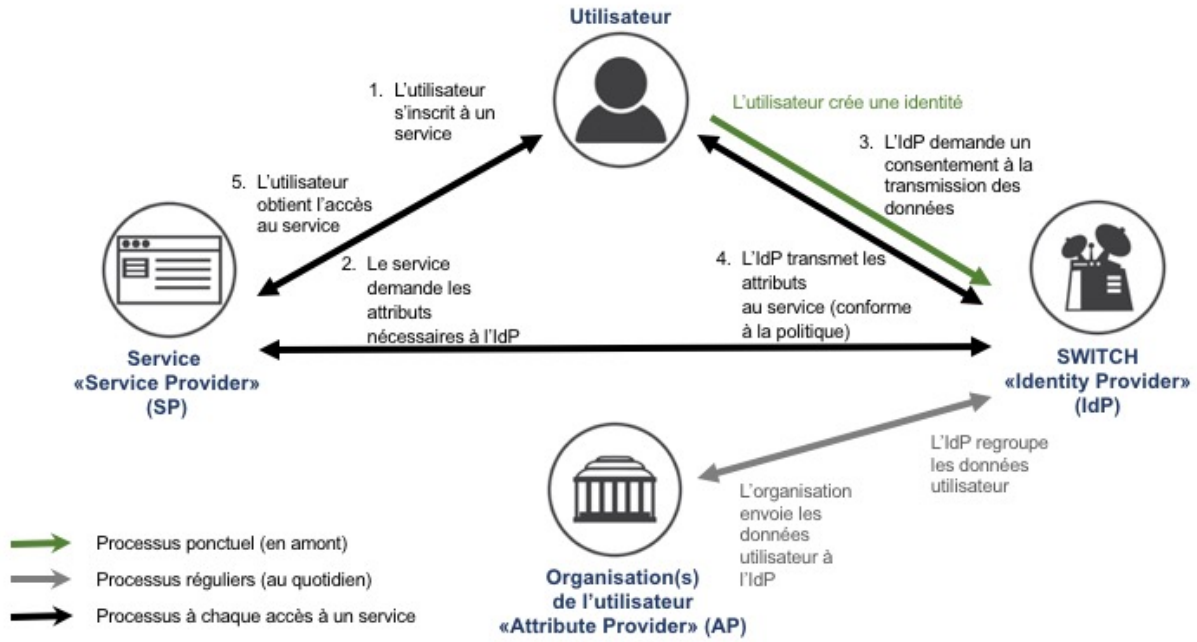
L'identifiant n'est pas affiché pour des raisons de sécurité.

4.3 Quelles données sont stockées dans un compte SWITCH edu-ID?

Le compte d'un utilisateur contient son identité de base et – le cas échéant – ses affiliations à des organisations («identités d'organisation»). Les données des affiliations actives sont transmises à SWITCH par les organisations. Il peut s'agir de tous les attributs qu'une organisation utilise ou seulement d'une partie (en fonction de la validation par l'organisation). Des informations relatives aux affiliations anciennes sont ajoutées à l'identité de base si une personne sort d'une organisation (cf. note de bas de page 3). Le niveau de qualité des divers attributs est également visible dans le compte.



4.4 À quoi les flux de données ressemblent-ils?



L'identité de base est créée lors de la création du compte. S'il existe des affiliations actives d'un utilisateur, elles sont regroupées chez SWITCH. Si un utilisateur a accès à un service (1), le service demande les attributs requis à l'IdP central de SWITCH (2). En conséquence, l'IdP demande à l'utilisateur s'il consent au transfert de données à ce service (3). Si l'utilisateur donne son consentement, l'IdP central transfère au service (4) les attributs nécessaires de manière conforme à la politique et l'utilisateur reçoit l'accès au service (5). L'utilisateur peut définir s'il souhaite donner son

consentement à chaque accès à un certain service ou uniquement lorsque des attributs ont été modifiés.

4.5 Dans quels processus SWITCH traite-t-elle quelles données?

Les données utilisateur sont enregistrées sous la forme d'attributs. À un attribut appartient une indication de statut qui indique la qualité de l'attribut, ainsi qu'une date (de création ou de modification). La plupart des données enregistrées peuvent être consultées dans le compte edu-ID de l'utilisateur. En plus, l'historique (des modifications) est enregistré et certains processus et actions sont journalisés si ceci est nécessaire pour l'exploitation (p. ex. traçabilité des actions qui entraînent des erreurs; administration de preuves en cas d'abus).

- Pour la **création manuelle d'un compte**, des données déclarées par l'utilisateur lui-même, comme le nom, le prénom, l'adresse, la date de naissance, au moins une adresse e-mail vérifiée et un mot de passe crypté, sont enregistrées.

- Lors de la **création d'un compte edu-ID sur la base d'un compte AAI** ou lors de la **mise en relation avec un compte AAI existant ou avec un compte d'une organisation**, les attributs du compte concerné sont repris par l'organisation dans un compte edu-ID. De plus, l'identifiant que l'organisation utilise est enregistré.

- Lors de la **vérification d'attributs** (nécessaire pour l'accès à certains services; vérification initiée si nécessaire), des attributs vérifiés comme des adresses e-mail contrôlées (qui peuvent tous être utilisés pour la connexion), des numéros de téléphone mobile contrôlés ou une adresse de résidence vérifiée sont stockés (d'autres contrôles peuvent être prévus à l'avenir). L'utilisateur fournit et enregistre lui-même ces données.

- Pour la mise en relation d'un compte avec un **ORCID**, l'utilisateur enregistre chez SWITCH son identifiant ORCID. Il est émis par https://orcid.org/.

- En cas de **modifications**, les attributs modifiés sont stockés chez SWITCH. Ils peuvent provenir de chaque organisme autorisé qui peut émettre des attributs pour un utilisateur au sein de la fédération (utilisateur, services spéciaux, organisations agissant en tant qu'attribute provider).

- En cas de suppression d'une affiliation active, SWITCH crée une copie de cette «current affiliation» et l'enregistre en tant que «**former affiliation**» (affiliation ancienne) avec une date de fin dans le compte de l'utilisateur. Une affiliation ancienne est uniquement utilisée dans un extended attribute model et est donnée uniquement aux services (p. ex. une application d'enregistrement d'un portail Alumni).

- Chez SWITCH, il est également enregistré quand et sur quel service une **connexion** d'un utilisateur a lieu. Ces informations sont évaluées à des fins statistiques (de manière anonymisée) par service et par organisation. En outre, elles servent à pouvoir résoudre des problèmes qui peuvent survenir en cas de **correction de doublons** en informant les services qu'un utilisateur a utilisés de l'association des comptes et du nouvel identifiant. Afin que les utilisateurs puissent se désinscrire de divers services, SWITCH doit également saisir à quels services un utilisateur est actuellement inscrit (single logout).

- L'attribute provider d'organisations ou certains services autorisés peuvent stocker **des attributs supplémentaires** (p. ex. sous la forme d'entitlements ou d'appartenances à des groupes) chez SWITCH, p. ex. pour permettre à un utilisateur l'accès à des contenus de bibliothèques.

- Pour l'**assistance**, SWITCH enregistre des contenus d'e-mails qui arrivent généralement sous la forme de tickets. Ces tickets contenant des requêtes d'utilisateurs sont enregistrés du fait que les journaux de processus y font référence dans edu-ID, p. ex. lorsqu'une identité doit être associée ou effacée.

4.6 Quels rôles SWITCH, les organisations et les utilisateurs finaux ont-ils?

Pour l'**usage A**, SWITCH est considérée comme «**processeur de données**» des organisations. Les organisations sont considérées comme les «**responsables**» au sens de la loi. Les utilisateurs finaux, donc les personnes concernées qui utilisent SWITCH edu-ID (étudiants, collaborateurs etc.), sont des «**sujets de données**».

Pour l'**usage B**, les organisations sont considérées, selon SWITCH, comme **processeur de données des personnes concernées** (voir à ce sujet plus d'informations au chiffre 4.8 ci-dessous). SWITCH est **sous-processeur de données**.

4.7 Quelles sont les obligations de SWITCH en tant que processeur de données?

En tant que processeur de données, SWITCH doit uniquement traiter des données personnelles de la manière dont les organisations ont elles-mêmes le droit de le faire (art. 10 a LPD). En tant que processeur de données, SWITCH est soumise p. ex. à toutes les **obligations de secret professionnel** applicables à l'organisation et aux autres obligations de confidentialité par rapport aux données traitées. SWITCH engage son personnel par écrit à la confidentialité. De plus, SWITCH s'engage contractuellement à **traiter les données personnelles uniquement selon les directives des organisations**.

Les organisations sont de surcroît contractuellement habilitées à **contrôler** elles-mêmes le respect chez SWITCH des dispositions relevant du droit sur la protection des données, ou à le faire contrôler par un tiers, au nom et pour le compte de l'organisation. Par ailleurs, le pouvoir de surveillance d'éventuels délégués cantonaux à la protection des données peut s'appliquer à SWITCH en sa qualité de processeur de données.

SWITCH garantit également de manière contractuelle que SWITCH supprime automatiquement les affiliations actives après la sortie d'une organisation de la fédération AAI, sans en conserver de copie, et que SWITCH confirme sur demande un tel effacement. De même, SWITCH supprime au cas par cas des affiliations actives sur sommation de l'organisation sans qu'une affiliation ancienne ne soit créée ou qu'une copie de l'affiliation ne soit conservée. L'effacement est confirmé sur demande.

4.8 Quelles sont les obligations des organisations en tant que responsables?

En tant que responsables, les organisations doivent **contrôler** que tous les **principes de traitement et d'autres principes sont observés** lors du traitement de données personnelles. Ceci s'appliquait déjà à la prestation de service SWITCHaai et à la fédération AAI sur lesquels SWITCH edu-ID est basé. Les principes qui doivent être observés et **la manière dont SWITCH veille à leur respect** sont présentés ci-après.

- **Principe de la proportionnalité (p. ex. art. 4 al. 2 LPD)**
  Les données ne peuvent être traitées que de manière proportionnée. Le règlement européen relatif à la protection des données prévoit le principe de **minimisation des données**. Ceci signifie surtout que seules les données nécessaires au fonctionnement de la prestation de service peuvent être collectées et que les données ne peuvent être conservées que pendant la durée nécessaire. Dans SWITCH edu-ID, seuls les attributs qui sont nécessaires au fonctionnement de la prestation de service sont traités. En conséquence, seuls les attributs dont les services ont besoin pour le fonctionnement de leur prestation de service sont transmis aux services.

- **Principe de la limitation à une finalité spécifique (p. ex. art. 4 al. 3 LPD)**
  Les données personnelles peuvent uniquement être traitées dans la finalité qui a été **indiquée** lors de la collecte de données, qui est **évidente** en fonction des circonstances ou qui est **prévue par la loi**. SWITCH garantit que les attributs sont uniquement traités dans les finalités qui figurent dans la description des services. En particulier, aucune donnée ne sera utilisée à des fins publicitaires ou marketing ou revendue à un tiers.

- **Principe de la reconnaissabilité (p. ex. art. 4 al. 4 LPD), devoir d'information (p. ex. art. 17 ss. P-LPD, art. 13, 14 RGPD)**
  La collecte de données personnelles et notamment la finalité de leur traitement doivent être **reconnaissables pour la personne concernée**. Dans la description des services et dans les conditions d'utilisation, SWITCH énonce de manière transparente et en des termes facilement compréhensibles les finalités pour lesquelles les données des utilisateurs sont utilisées. Chaque utilisateur doit accepter les conditions d'utilisation lors de la création d'un compte. SWITCH assume donc pour les hautes écoles le devoir d'information à l'égard des personnes concernées.

- **Principe de la légalité (p. ex. art. 17 LPD)**
  - Par principe, les organes fédéraux (ETH, EPFL) et les organisations cantonales ont besoin d'une **base légale** pour le traitement des données personnelles. Pour la transmission de données personnelles à des tiers (p. ex. à SWITCH), un consentement suffit dans la plupart des cantons (pour un complément d'information sur le transfert de données, voir chiffre 5.1 c dans ce qui suit).
  - Pour le traitement de données dans les **finalités de l'administration des hautes écoles («finalité A»)**, les hautes écoles disposent d'une base légale suffisante. Pour le traitement de données dans les **finalités des utilisateurs («finalité B»)**, les hautes écoles ne disposent certes pas d'une base légale suffisante, mais les **hautes écoles opèrent pour le compte des utilisateurs**, si bien que la nécessité de la base légale est annulée.

- Avant le transfert de données par les hautes écoles à SWITCH et par SWITCH aux différents services, SWITCH demande toujours le **consentement des utilisateurs finaux**. Le consentement représente un motif justificatif suffisant pour la transmission des attributs. Comme les hautes écoles ne disposent plus d'une base légale pour avoir le droit de conserver les données des **utilisateurs finaux après leur sortie**, les utilisateurs finaux sont conservés sous la forme d'une «former affiliation» de manière centralisée chez SWITCH en cas de sortie d'un utilisateur de l'organisation. Une telle affiliation (inactive) renferme une partie des attributs de l'affiliation ancienne et ne peut plus être modifiée après sa création. **En tant que fondation de droit privé, SWITCH n'a pas besoin d'une base légale pour la conservation centralisée des attributs.**

- **Exactitude des données (p. ex. art. 5 LPD)**

  Celui qui traite des données personnelles doit s'assurer de leur exactitude. Il doit prendre toutes les mesures adéquates afin que soient rectifiées ou effacées les données qui sont inexactes ou incomplètes par rapport à la finalité de leur collecte ou de leur traitement. SWITCH contrôle la validité des adresses e-mail et des numéros de téléphone mobile stockés dans l'identité de base. La qualité des attributs est également mise à la disposition en tant qu'information, par exemple pour des services. Grâce à différentes méthodes de mise à jour des attributs, il est garanti que les attributs que SWITCH traite sont actuels. De plus, l'exactitude des attributs «nom», «prénom» et «adresse e-mail» a généralement été vérifiée par la haute école avant qu'elle ne les transmette à SWITCH. La nouvelle «loi e-ID» ouvre la possibilité pour SWITCH d'obtenir des attributs qualifiés de la part d'un organe qualifié, donc p. ex. un nom qui a été contrôlé par un organisme de contrôle au moyen d'un contrôle d'identité. Enfin, SWITCH contrôle la présence de doublons sur les comptes existants de manière continue, ce qui sert également à l'exactitude des données existantes. Dans l'interface utilisateur, les adresses de contact des organisations sont portées à la connaissance des utilisateurs, et c'est à cet endroit qu'ils peuvent demander la correction d'éventuelles données d'une affiliation qui sont inexactes ou qui ne sont plus d'actualité.

- **Communication transfrontalière (p. ex. art. 6 LPD)**

  - Des services auxquels les utilisateurs accèdent avec l'edu-ID peuvent se trouver à l'étranger (dans le monde entier). Une communication de données personnelles dans des «pays tiers non sûrs», comme p. ex. les États-Unis (cf. la liste des États du PFPDT), est autorisée si le consentement de la personne concernée a été obtenu dans un cas particulier ou si le respect d'un niveau adéquat de protection des données est garanti d'une autre manière. En tant qu'Identity Provider, SWITCH demande, au moins à la première utilisation d'un service, le consentement des utilisateurs avant que leurs données soient transmises à des fournisseurs de services. L'utilisateur peut décider lui-même s'il souhaite que son consentement lui soit demandé à chaque accès à un service ou uniquement lorsque ses attributs sont modifiés.

  - Les partenaires de la fédération SWITCHaai peuvent proposer leurs services depuis n'importe quel pays. Chaque partenaire de la fédération est lié par un contrat conclu avec SWITCH dans le cadre légal de SWITCH edu-ID.

- La fédération SWITCHaai est liée au cadre de la politique du service d'interfédération eduGAIN de GÉANT. Ce cadre régit les relations avec les services qui sont liés par analogie avec d'autres fédérations dans le monde entier[5].

- **Sécurité des données (p. ex. art. 7 LPD)**
  Les données personnelles doivent être protégées contre un **traitement non autorisé** par des mesures techniques et organisationnelles appropriées. SWITCH assume toutes les mesures raisonnables pour garantir à tout moment la sécurité des données conformément à l'état reconnu de la technique. Dans le cas de SWITCH edu-ID, ceci inclut (voir la description du service):
  - des mesures structurelles et des restrictions d'accès à l'infrastructure du serveur
  - un règlement relatif à l'accès (concept utilisateur, firewall et dispositif similaire)
  - une maintenance régulière du serveur
  - une surveillance automatisée des services
  - un concept d'exploitation redondant et une création de sauvegardes pour une protection contre des pertes de données
  - un codage des données et une signature lors de la transmission de données
  - la promotion d'une culture de tempérance lors de la transmission de données au sein de la fédération
  - l'implication de l'utilisateur final dans les processus qui concernent ses données
  - la sensibilisation du personnel à des questions de protection des données à travers des ateliers
  - des règlements et des instructions
  - des contrats

  L'organisation a le droit de se faire expliquer dans le détail les processus opérationnels correspondants.

- **Sauvegarde des droits de personnes concernées**
  Les responsables (donc les hautes écoles) doivent s'assurer que les personnes concernées peuvent exercer tous leurs droits. En font partie le **droit d'accès** (art. 8 LPD, art. 23 ss. P-LPD, art. 15 RGPD), le **droit de rectification** (art. 5 al. 5 P-LPD, art. 16 RGPD), le **droit à l'effacement** (art. 5 al. 5 P-LPD, art. 17 RGPD), le **droit d'opposition** (art. 26 al. 2 lit. b P-LPD, art. 21 RGPD), le droit à la **limitation du traitement** (art. 18 RGPD) et le droit à la **portabilité des données** (art. 20 RGPD). SWITCH assiste les hautes écoles dans la garantie de ces droits. En conséquence, les organisations répondent certes elles-mêmes aux demandes de renseignement, mais SWITCH fournit aux hautes écoles toutes les informations nécessaires sur première demande. SWITCH effectue également les corrections d'attributs sur demande. De plus, SWITCH a mis en place un mécanisme qui permet à une personne concernée l'effacement de ses données lorsqu'elle le souhaite (s'il n'existe aucune affiliation active à une organisation). Enfin, SWITCH peut restituer les attributs sur demande dans un format transférable et lisible par une machine. Pour plus d'informations sur le droit à l'effacement, voir au chiffre 4.7 ci-dessous et au chiffre 5.3 a) ci-dessous.

[5] voir la description du service SWITCH edu-ID https://www.switch.ch/edu-id/terms/.

5 Questions aux responsables de la protection des données

Depuis 2015, SWITCH a demandé à plusieurs responsables de la protection des données de lui faire part de leurs commentaires sur l'architecture et les processus de SWITCH edu-ID, du fait que d'importantes modifications se sont produites par rapport à SWITCHaai. Trois responsables cantonaux de la protection des données (Fribourg, Lucerne, Zurich) ont exprimé leur position par rapport aux questions de SWITCH. Les questions de SWITCH, les réponses des responsables de la protection des données, les compléments d'information apportés par SWITCH et une conclusion sont présentés dans ce qui suit.

5.1 Premier usage: utilisation de SWITCH edu-ID dans le cadre de l'administration des hautes écoles (finalité A)

a) **Base légale**
Pour l'usage A, il s'agit pour SWITCH edu-ID d'un nouveau *moyen* de traitement qui sert aux *finalités* de traitement de l'administration des hautes écoles déjà poursuivies. Par conséquent, SWITCH edu-ID est soumis aux mêmes exigences de l'art. 4 de la LPD FR, voire au § 5 de la LPD LU, voire au § 8 al. 1 de la loi sur l'information et la protection des données ZH que le traitement général de données dans le cadre de l'administration des hautes écoles.

Êtes-vous d'accord avec le fait que SWITCH edu-ID est **couvert par une base légale déjà existante**, ou que ceci peut être justifié tout comme l'activité précédente de l'administration des hautes écoles si les dispositions relatives à l'accomplissement des tâches de la haute école le prévoient?

Réponse:
*Oui, du fait qu'avec edu-ID seules des **données communes** comme le nom, le prénom, l'adresse e-mail et éventuellement la date de naissance sont saisies et qu'il n'existe aucun profil de personnalité, le traitement des données dans le cadre de l'edu-ID aux fins de l'administration des hautes écoles peut être classé dans les bases légales existantes et aucune base légale supplémentaire n'est requise. Les délégués à la protection des données ZH et FR sont également de ce point de vue, comme indiqué ci-après. La raison pour laquelle le délégué à la protection des données LU demande de manière générale une base légale supplémentaire pour l'utilisation de SWITCH edu-ID n'est pas justifiée et n'est pas non plus fondée.*

Détails sur les réponses des responsables de la protection des données:
Dans la mesure où des données personnelles comme le prénom, le nom, l'adresse e-mail ou d'autres données personnelles non sensibles sont saisies et traitées avec le nouveau processus d'authentification, les délégués à la protection des données ZH et FR sont d'avis que ce traitement peut être classé dans les dispositions légales existantes. Toutefois, si des données sensibles ou nécessitant une protection particulière sont saisies ou si les données personnelles collectées sont liées à d'autres caractéristiques ou à d'autres informations, créant ainsi des informations sensibles ou même des profils de personnalité, il est indispensable de s'appuyer sur une base légale formelle.

Il est d'avis du délégué à la protection des données LU que l'utilisation de SWITCH edu-ID nécessite de manière générale une base légale supplémentaire.

Complément d'informations apporté par SWITCH:
Actuellement, aucune donnée sensible n'est saisie avec l'edu-ID (donc par exemple des données sur les opinions religieuses, philosophiques ou politiques ou sur la santé, la vie privée ou l'appartenance à une race ainsi que des données génétiques ou biométriques qui identifient clairement une personne physique).

Des données ou des profils sensibles sont éventuellement présents dans les services (par exemple les données d'un système de bibliothèque sur le comportement de lecture d'un étudiant) ou dans les hautes écoles elles-mêmes (p. ex. les dossiers médicaux des patients à l'hôpital universitaire de Zurich). Toutefois, SWITCH ne dispose pas de ces données.

De même, SWITCH ne fait **pas de «profilage»** (le «profilage» est la valorisation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée, notamment pour analyser ou pronostiquer la performance de travail, la situation financière, la santé, le comportement, les préférences, le domicile ou la mobilité, voir à ce sujet le chiffre 5.4 ci-dessous.)

b) **Traitement de données sur mandat**
SWITCH opère-t-elle en qualité de processeur de données dans le rôle d'exploitant du service qui reçoit et transmet des attributs pour le compte des hautes écoles ou qui conserve de manière centralisée des attributs pour les besoins des hautes écoles? Quelles exigences SWITCH doit-elle respecter en ce qui concerne les traitements de données pour le compte des hautes écoles?

Réponse:
Oui, SWITCH opère par principe en qualité de processeur de données. Par analogie, il faut s'assurer que ***toutes les dispositions légales relatives au traitement de données sur mandat sont observées****. SWITCH garantit que toutes les dispositions légales relatives au traitement de données sur mandat sont observées. Ceci englobe la conclusion d'un contrat avec les hautes écoles (qui se compose d'une description des prestations, d'un règlement relatif aux prestations et de tarifs) qui contient toutes les informations nécessaires. C'est notamment au chiffre 7.2 du règlement relatif aux prestations que SWITCH garantit que les données personnelles sont traitées uniquement dans les finalités convenues et selon les directives indiquées dans la description des services, que SWITCH est soumise aux obligations de secret professionnel applicables à l'organisation et qu'elle engage par écrit son propre personnel au respect de la confidentialité. De plus, SWITCH s'engage à assister les organisations dans le respect des dispositions relevant du droit sur la protection des données qui leur sont applicables.*

De plus, SWITCH garantit que des ***mesures techniques et organisationnelles appropriées relatives à la protection des données*** *sont prises (voir chiffre 7.2 lit. b du règlement relatif aux prestations). Avec la description détaillée des prestations et les conditions d'utilisation qui sont remises à chaque administration d'une haute école et qui doivent être de plus «cliquées» par chaque utilisateur final lors de la création d'un compte edu-ID, SWITCH garantit également*

*que les personnes concernées et l'administration des hautes écoles sont **informées de façon intégrale et transparente sur l'edu-ID et sur ses usages actuels et potentiels**. Selon la loi, ce serait en fait le devoir du responsable (de la haute école) et non du responsable du traitement (SWITCH) d'informer les personnes concernées sur l'utilisation des données dans le cadre de l'edu-ID (voir art. 18a LPD, art. 17 P-LPD). SWITCH décharge les hautes écoles de ce devoir d'information vis-à-vis des personnes concernées.*

Détails sur les réponses des responsables de la protection des données:
Les trois responsables de la protection des données retiennent qu'il s'agit d'un «**traitement sur mandat**» dans la mesure où le traitement des attributs se fait pour le compte des hautes écoles dans les finalités de l'administration des hautes écoles. Dans un tel cas, la haute école est «responsable» et SWITCH «processeur de données». Les **dispositions légales applicables à un traitement des données sur mandat doivent être respectées**. Ceci englobe la conclusion d'un contrat qui contient notamment le droit de donner des instructions dont dispose la haute école ainsi que les dispositions relatives à la confidentialité. SWITCH a uniquement le droit de traiter des données de la manière dont la haute école le ferait elle-même. En tant que mandataire, SWITCH est tenue de respecter les bases légales applicables aux hautes écoles.

Le délégué à la protection des données ZH retient également que la saisie et le traitement centralisés de toutes les informations d'authentification pour toute la Suisse des hautes écoles en Suisse entraîneraient, du point de vue du droit de la protection des données, des risques plus élevés pour les personnes concernées dont il faut tenir compte lors de la mise en œuvre des mesures organisationnelles et techniques. Le délégué à la protection des données LU signale également le risque en matière de droit de la protection des données qui est supérieur par rapport à SWITCHaai (notamment ceux qui résultent des possibilités de connexion supplémentaires, du nombre accru d'attributs ainsi que de la plus grande durée de vie des attributs) et note que les étudiants et l'administration des hautes écoles doivent être **informés de manière intégrale et transparente sur l'edu-ID et ses usages (potentiels)**.

c) **Exigences relatives au transfert de données**
Quelles exigences doivent être observées par les hautes écoles en ce qui concerne le transfert d'attributs à SWITCH? Outre une réglementation contractuelle en conformité avec la protection des données applicable entre SWITCH et la haute école concernée, existe-t-il d'autres conditions qui doivent être créées?

Réponse:
*Dans le cas de la **finalité A** (administration des hautes écoles), un **contrat suffisant** est nécessaire entre SWITCH et les hautes écoles, et il en existe bien un (voir à ce sujet le chiffre 5.1 b) ci-dessus). Dans le cas de la **finalité B** (finalités de l'utilisateur), un **consentement de l'utilisateur** est requis. SWITCH obtient un tel consentement à chaque communication de données. Dès lors qu'un utilisateur souhaite accéder à un service, il lui est montré de manière transparente et facilement compréhensible les attributs dont le service a besoin, et les attributs sont uniquement transmis si l'utilisateur consent à leur transfert («user consent»).*

Détails sur les réponses des responsables de la protection des données:
Le délégué à la protection des données ZH indique qu'une distinction doit être faite entre les finalités pour lesquelles des données sont communiquées par les hautes écoles à SWITCH. Si une transmission est effectuée dans les **finalités de l'administration des hautes écoles (finalité A)**, il s'agit d'un traitement de données sur mandat, et c'est pourquoi seul un contrat est nécessaire entre SWITCH et les hautes écoles (voir à ce sujet lit. b ci-dessus).

Si toutefois une transmission se fait pour **d'autres finalités**, à savoir pour la **finalité B** (l'utilisateur a accès à une prestation de service avec l'edu-ID qui est proposée par un service hors du secteur universitaire), ceci est uniquement possible dans les conditions prévues aux §§ 16 et 17 de la loi sur l'information et la protection des données («communication de données personnelles»), à savoir si une base juridique l'autorise ou s'il existe un **consentement de la personne concernée dans un cas particulier**.

En réponse à cette question, le délégué à la protection des données FR mentionne que SWITCH ne doit pas traiter les données personnelles pour une autre finalité que pour l'administration des hautes écoles et que SWITCH ne doit pas communiquer des données à des tiers.

Complément d'informations apporté par SWITCH:
Les propos du délégué à la protection des données FR selon lesquels SWITCH ne doit pas utiliser les données pour l'usage B et selon lesquels une transmission à des tiers est interdite ne sont pas fondés. La loi du canton de Fribourg prévoit expressément – tout comme la loi du canton de Zurich – qu'un **transfert de données est autorisé avec le consentement de l'utilisateur**, c'est-à-dire **indépendamment de la finalité**. De manière spécifique, il est important:

- que les utilisateurs soient informés de manière transparente sur l'usage,
- qu'ils consentent au transfert et
- que les données ne soient pas utilisées dans d'autres finalités que celles qui ont été communiquées à l'utilisateur.

Ceci est évidemment respecté par l'edu-ID (voir également à ce sujet les propos sur la finalité aux chiffres 4.1 et 4.8 ci-dessus).

d) **Saisie d'attributs par la haute école**
En ce qui concerne la saisie initiale des attributs des utilisateurs par la haute école par rapport aux processus normaux de l'administration des hautes écoles, existe-t-il d'autres conditions qui doivent être respectées?

Réponse:
Non, il n'existe ***pas de conditions supplémentaires que les hautes écoles doivent respecter lors de la saisie initiale des attributs.***

Détails sur les réponses des responsables de la protection des données:
Le délégué à la protection des données ZH déclare que la saisie se fait sur la base des **procédures normales dans le cadre des bases juridiques en vigueur**. Il est notamment important que les mesures relatives à la sécurité de l'information soient mises en œuvre. Le

délégué à la protection des données FR constate que l'université doit garantir le fait que SWITCH traite uniquement les données de la manière dont l'université devrait le faire elle-même. L'université doit donner les instructions correspondantes et s'en assurer contractuellement. Le délégué à la protection des données LU énonce uniquement que les hautes écoles dans le canton de Lucerne devraient respecter les exigences des §§ 13 et 16 de la loi informatique et libertés (dispositions relatives à l'externalisation de prestations de service dans le domaine de l'informatique).

Complément d'informations apporté par SWITCH:
SWITCH partage l'opinion du délégué à la protection des données ZH selon laquelle la saisie initiale des attributs des utilisateurs peut être classée dans les bases juridiques en vigueur. En conséquence, il faut partir du principe qu'aucune autre condition n'est à observer pour la saisie initiale des attributs par les hautes écoles. C'est l'affaire des hautes écoles de s'assurer que des mesures de sécurité appropriées sont mises en œuvre lors de la saisie initiale des attributs.
Les propos des délégués à la protection des données FR et LU n'ont rien à voir avec la question posée. SWITCH est consciente du fait qu'elle a uniquement le droit de traiter les données de la manière dont les hautes écoles pourraient le faire elles-mêmes et s'y tient. De même, SWITCH respecte toutes les dispositions légales en rapport avec l'externalisation de traitements de données (voir à ce sujet le chiffre 5.1. b) ci-dessus).

5.2 Deuxième usage: utilisation de SWITCH edu-ID dans les finalités de l'utilisateur (finalité B)

L'utilisation d'edu-ID dans les finalités de l'utilisateur peut se faire en même temps que pour le premier usage (chiffre 5.1 ci-dessus). Ceci serait le cas si un étudiant inscrit dans une haute école utilise edu-ID pour acheter en ligne un livre d'une édition scientifique en bénéficiant d'un avantage. Toutefois, elle peut se produire également de manière différée: il serait ici imaginable qu'un utilisateur quitte la haute école mais continue d'utiliser edu-ID, par exemple pour gérer ses titres d'études et les documents de son curriculum vitae.
Dans ce contexte, les questions suivantes se posent:

a) **Rôle de la haute école**
Peut-on supposer que le **rôle de la haute école vis-à-vis de l'utilisateur est celui de simple processeur de données** et que la nécessité d'une base légale énoncée à l'art. 17 al. 1 LPD ou au § 8 de la loi sur l'information et la protection des données ne s'applique pas (du fait que la haute école ne décide pas elle-même dans ce cas de la finalité du traitement des données)?

Réponse:
Tout comme les délégués à la protection des données ZH et FR, SWITCH est d'avis que l'utilisation d'edu-ID est autorisée pour la finalité B avec le ***consentement des utilisateurs*** *et qu'****aucune base légale supplémentaire*** *n'est nécessaire. Comme* ***motif justificatif d'un traitement des données, une base légale OU un consentement suffit****.*

Détails sur les réponses des responsables de la protection des données:
Les délégués à la protection des données ZH et FR ne s'expriment pas sur la question de savoir si la haute école est alors un processeur de données des utilisateurs. Ils déclarent seulement que le transfert d'attributs à SWITCH aux fins d'une transmission aux services est, du point de vue des hautes écoles, une communication de données qui nécessite le consentement des utilisateurs au cas par cas ou alors une base légale. Le consentement ne doit pas obligatoirement être demandé par les hautes écoles, mais il peut également être demandé par SWITCH.

De plus, le délégué à la protection des données FR mentionne que les universités n'ont aucune base légale pour demander un consentement auprès des étudiants. Le délégué à la protection des données LU annonce que selon lui la finalité B n'est pas un traitement de données sur mandat par les hautes écoles, mais un traitement de données dans le cadre de missions supplémentaires des hautes écoles qui doit être légalement régi de manière explicite. Le délégué à la protection des données LU demande donc une nouvelle base légale afin que SWITCH edu-ID puisse être utilisé pour la finalité B (en outre, il demande une nouvelle base légale afin qu'edu-ID puisse être utilisé pour la finalité A, voir à ce sujet le chiffre 5.1 a) ci-dessus).

Complément d'informations apporté par SWITCH:
Les propos du délégué à la protection des données FR selon lesquels les universités n'ont aucune base légale pour demander un consentement ne sont pas fondés. Il n'est pas besoin d'une base légale pour demander un consentement.

De plus, il convient d'observer que par rapport à la situation actuelle, **aucune donnée supplémentaire n'est générée** avec edu-ID et qu'aucune **nouvelle finalité de traitement** n'est poursuivie. Si un étudiant souhaite bénéficier aujourd'hui d'un abonnement à un magazine à un tarif préférentiel et s'il envoie à cette fin une copie de sa carte d'étudiant à une maison d'édition, cette dernière saisit également les données de l'étudiant. Il en est de même avec les services internes aux hautes écoles: Si un étudiant souhaite aujourd'hui emprunter un livre, il doit également justifier de son identité auprès du service de bibliothèque et ses données sont alors saisies par le service de bibliothèque. Les hautes écoles mettent à la disposition de leurs membres/étudiants un moyen d'identification avec la carte d'ayant droit. Ceci se fait par défaut pour l'achat de services des hautes écoles et en dehors du contexte universitaire (finalité B) sans qu'il n'existe une certaine base légale à ce titre. La différence en ce qui concerne la légitimation dans le cas de l'utilisation de SWITCH edu-ID réside dans le fait que les données de l'utilisateur sont **transmises électroniquement** à un service de bibliothèque ou à une maison d'édition, au lieu d'une saisie manuelle. Dans ce processus électronique, moins de données sont transmises que dans une procédure «manuelle» car la **minimisation des données** est définie contractuellement et est contrôlée par les administrateurs des organisations et des services. Seules les données nécessaires à l'exploitation sont transférées.

Exigences imposées à une haute école agissant en qualité de processeur de données sur mandat

b) **Mesures**
La haute école doit-elle prendre des mesures pour justifier la conservation des données (tout comme pour le premier usage A) pour ce deuxième usage (B)?

Réponse:
*Non. SWITCH obtient le **consentement des utilisateurs** avant chaque communication de données. D'autres mesures ne doivent pas être prises.*

Détails sur les réponses des responsables de la protection des données:
Les délégués à la protection des données ZH et FR ne s'expriment pas sur la question de savoir si certaines mesures doivent être prises pour la conservation des données dans les hautes écoles. Ils annoncent uniquement que le consentement des utilisateurs doit être demandé au cas par cas avant une communication des données à SWITCH. Le délégué à la protection des données LU demande une base légale de manière générale pour la conservation des données dans les universités.

Complément d'informations apporté par SWITCH:
SWITCH part du principe qu'aucune mesure supplémentaire n'est requise étant donné que les données doivent être enregistrées d'une part déjà pour le premier usage (A) dans la haute école et que l'utilisateur est d'autre part libre de ne pas utiliser du tout edu-ID lui-même pour le deuxième usage (B).

c) **Consentement pour une poursuite de l'utilisation en cas de sortie**
Sous l'angle du droit relatif à la protection des données, est-ce qu'il est suffisant de demander à l'utilisateur, avant sa sortie de la haute école, s'il souhaite continuer à utiliser SWITCH edu-ID pour justifier le transfert de ses attributs à SWITCH?

Réponse:
*Oui, sous l'angle du droit relatif à la protection des données, il est suffisant de demander à l'utilisateur, **avant sa sortie de la haute école**, s'il souhaite continuer à utiliser SWITCH edu-ID. Avec ce consentement, la poursuite du stockage des attributs chez SWITCH est autorisée par le droit relatif à la protection des données.*

Détails sur les réponses des responsables de la protection des données:
Tous les responsables de la protection des données ont répondu à cette question par l'affirmative. Le délégué à la protection des données ajoute que les utilisateurs doivent être informés au préalable (avant la sortie) des conséquences de manière transparente.

d) **Consentement pour une poursuite de l'utilisation au moment de la sortie**
Est-il autorisé de concevoir ce consentement dès la création d'un compte edu-ID en tant qu'opt-out – en d'autres termes le fait que le compte de l'utilisateur soit transféré dans la mesure où l'utilisateur n'exprime pas à SWITCH qu'il ne souhaite plus poursuivre l'utilisation de son compte?

Réponse:
*Un **opt-out** relatif à la poursuite de l'utilisation de comptes SWITCH edu-ID après la sortie d'une haute école est par principe autorisé.*

Détails sur les réponses des responsables de la protection des données:
Les délégués à la protection des données ZH et FR considèrent un opt-out comme quelque chose de possible, même s'ils préfèrent un opt-in en ce qui concerne le règlement européen relatif à la protection des données. Le délégué à la protection des données LU demande un opt-in. Il justifie sa réponse par le fait que les comptes sont des profils de personnalité, voire des données sensibles.

Complément d'informations apporté par SWITCH:
Quant à la question de savoir si la demande du consentement peut être conçue sous la forme d'un opt-out, il importe de savoir si l'on a recours à loi suisse sur la protection des données pour les personnes physiques ou au RGPD comme norme. De surcroît, il est essentiel de connaître la manière dont la «solution opt-out» est concrètement conçue. Les cases déjà cochées continuent d'être considérées en Suisse comme un consentement valable si la case constitue l'objet d'une déclaration qui est soumise à une volonté claire de la personne concernée.

e) ***Garde et transmission d'attributs***
Comme dans la solution SWITCHaai précédente, un utilisateur SWITCH edu-ID peut dans un cas particulier décider de la transmission des attributs requis au service qu'il souhaite (indication des attributs souhaités par le service et possibilité d'une acceptation/d'un refus global en ce qui concerne tous les attributs listés).

Cette possibilité de contrôle dont dispose l'utilisateur peut-elle proposer, en guise d'alternative aux mesures énoncées précédemment, une justification au titre de la conservation des attributs par la haute école, la transmission des attributs à SWITCH ainsi que la transmission des attributs par SWITCH au service?

Réponse:
Le consentement de l'utilisateur est suffisant *pour justifier un stockage central des données et un transfert de données pour la finalité B. Au cours d'une relation avec une haute école, les hautes écoles agissent en qualité de* ***processeur des données de l'utilisateur****.*

Détails sur les réponses des responsables de la protection des données:
Les responsables de la protection des données ZH et FR s'entendent sur le fait que le **consentement suffit** pour une transmission des attributs à SWITCH et pour la transmission des attributs par SWITCH aux services. À ce sujet, le délégué à la protection des données LU est d'un autre avis; il demande une base légale – toutefois sans la motiver.

En ce qui concerne la conservation des attributs dans une haute école, le délégué à la protection des données ZH ne s'exprime pas sur le fait de savoir si le consentement présente un motif justificatif suffisant tant que dure la relation avec une haute école. Néanmoins, il déclare que le consentement ne présente pas un motif justificatif pour la conservation d'attributs par les hautes écoles après la fin de la relation avec une haute école.

Le délégué à la protection des données FR est d'avis que le consentement des utilisateurs ne sert en aucun cas de justification pour la conservation/garde de données par une haute école (indépendamment du fait que la relation avec une haute école existe encore ou non). Tout comme le délégué à la protection des données LU, il demande une base légale.

Complément d'informations apporté par SWITCH:
Après la cessation de la relation avec une haute école, les hautes écoles ne peuvent plus conserver chez elles les attributs à défaut d'une base légale. C'est pour cette raison que SWITCH a décidé de conserver les attributs chez elle de manière centralisée. En tant que fondation de droit privé, SWITCH n'a pas besoin d'une base légale pour stocker chez elle des attributs de manière centralisée. La seule chose nécessaire est le **consentement des utilisateurs** que SWITCH demande également (les dispositions correspondantes sont énoncées dans la description du service que les utilisateurs doivent accepter).

En ce qui concerne la conservation/garde de données par les hautes écoles pour la finalité B au cours d'une relation avec une haute école, SWITCH est d'avis que les hautes écoles sont les processeurs de données sur mandat des utilisateurs et qu'ainsi aucune base légale n'est nécessaire pour la saisie et la conservation des données (voir à ce sujet également le chiffre 4.8 ci-dessus).

5.3 Questions en rapport avec l'utilisation de SWITCH edu-ID sur une longue durée

Au cours d'une relation continue d'un utilisateur avec une organisation, des attributs de l'utilisateur sont stockés localement par l'organisation et transmis à SWITCH sous la forme d'une ou plusieurs «current affiliations» (voir la définition de «current affiliation» à la note de bas de page 2 plus haut). Une copie de ces affiliations actives est stockée de manière centralisée chez SWITCH qui agit en tant qu'exploitant du service. Après la sortie de la haute école par l'utilisateur, une affiliation active est transformée en une «former affiliation». Celle-ci contient une partie des attributs de l'ancienne «current affiliation» et est dotée en plus d'une date de fin. Si l'utilisateur souhaite poursuivre l'utilisation de son compte, cette information relative à une ancienne appartenance à l'organisation est conservée chez SWITCH pour pouvoir soutenir des processus qui sont en rapport avec les études valables une vie durant.

a) **Suppression d'un compte**
L'utilisateur doit-il avoir la possibilité de demander à SWITCH la suppression de son compte?

Réponse:
Oui. Les utilisateurs peuvent demander la suppression de leur compte à tout moment. Dès qu'il existe une affiliation à une organisation, SWITCH a toutefois le droit de supprimer le compte d'un utilisateur sur la base du contrat conclu avec l'organisation.

Détails sur les réponses des responsables de la protection des données:
Tous les responsables de la protection des données sont d'accord sur le fait que le **droit à l'autodétermination** relatif aux propres données englobe également le droit de faire effacer les données.

Complément d'informations apporté par SWITCH:
Tous les utilisateurs peuvent à tout moment modifier ou même supprimer eux-mêmes des attributs dans leur identité de base – à l'exception des données requises pour l'obtention du compte. Si les utilisateurs ne sont pas/plus immatriculés/engagés dans une organisation, ils ont la possibilité de faire supprimer complètement et à tout moment leur compte SWITCH edu-ID. Toutefois, il n'est pas possible qu'un étudiant/collaborateur supprime son compte SWITCH edu-ID au cours d'une relation avec une haute école, étant donné que les hautes écoles ont besoin de comptes SWITCH edu-ID pour leur propre administration (finalité A). Le compte est la condition impérative au fonctionnement des processus de gestion de l'identité et à l'authentification des utilisateurs dans les hautes écoles.

b) **Création d'un nouveau compte «vide»**
Est-il impérativement nécessaire que l'utilisateur ait la possibilité de créer un nouveau compte qui ne contient aucun ancien attribut provenant de son ancien compte ou est-il permis de refuser l'émission d'un deuxième compte en excluant d'anciens attributs?

Réponse:
Il est permis de refuser l'émission d'un deuxième edu-ID en excluant d'anciens attributs, du fait que les utilisateurs doivent avoir la possibilité de désactiver d'affiliations anciennes ou d'empêcher leur transmission s'ils le souhaitent. Dans des cas justifiés, il est possible de renoncer à l'association d'un ancien compte avec un nouveau compte «vide». L'ancien compte doit alors être supprimé.

Détails sur les réponses des responsables de la protection des données:
Le délégué à la protection des données ZH déclare que la haute école décide du processus de saisie des attributs. La seule chose importante est qu'il soit transparent, donc porté à la connaissance des utilisateurs. Le délégué à la protection des données LU note qu'il s'agit d'une question politique selon son point de vue. Enfin, il faut établir un équilibre entre le droit à l'autodétermination en matière d'information et le niveau d'exhaustivité des attributs nécessaire à une utilisation judicieuse par SWITCH edu-ID.

c) **Désactivation/suppression de comptes abandonnés**
Est-il nécessaire selon le droit relatif à la protection des données de contacter les titulaires de comptes non utilisés depuis longtemps après un certain délai (p. ex. au bout de 5 ans) et de savoir finalement si leurs comptes doivent encore être disponibles? Si l'utilisateur manifeste sa volonté de suppression ou s'il ne réagit pas à la demande de contact, est-il autorisé de retarder la suppression définitive de son identité d'une année supplémentaire (p. ex. avec un simple blocage de ses données mais sans suppression)?

Réponse:
Il est autorisé et judicieux que des comptes SWITCH edu-ID abandonnés soient désactivés dans un délai de 5 à 10 ans après la dernière utilisation et supprimés après une période de grâce d'une autre année.

Détails sur les réponses des responsables de la protection des données:
Le délégué à la protection des données LU considère cette réglementation comme judicieuse. Le délai proposé de 5 ans lui semble proportionnel et même une solution progressive avec une désactivation du profil dans une première phase et avec un effacement uniquement dans une

deuxième phase est possible et même judicieuse. Les délégués à la protection des données ZH et FR n'ont apporté aucune réponse à cette question car ils n'y avaient jamais été confrontés.

Complément d'informations apporté par SWITCH:
Compte tenu de l'objectif des études valables une vie durant, il est important pour SWITCH de garantir la possibilité d'utilisation des comptes même après de très longues interruptions. Une période de grâce doit assurer le fait que l'utilisateur puisse modifier ultérieurement son avis au cas où il termine une formation continue universitaire quelques années après ou s'il débute une autre activité dans un contexte universitaire.

Une période plus longue d'une durée allant jusqu'à 10 ans viendrait à l'encontre des hautes écoles. Dans ce cas, elles pourraient reconnaître d'anciens utilisateurs même après de très longues interruptions.

d) **Mise à jour des données**
d1) Pour la mise à jour périodique et automatique des données («attribute aggregator»), un nouveau consentement est-il requis ou part-on du principe qu'un consentement unique suffit?

Réponse:
*Un **consentement unique suffit**. Tout le reste n'aurait pas de sens et ne serait pas dans l'intérêt de l'utilisateur concerné. SWITCH demande les consentements des personnes concernées.*

Détails sur les réponses des responsables de la protection des données:
Aucune réponse n'a été faite à ce sujet.

d2) L'art. 5 LPD ou le § 7 al. 2 lit. b de la loi sur l'information et la protection des données peut-il être considéré comme motif justificatif pour les mises à jour périodiques et automatiques selon lequel les données doivent être exactes et mises à jour si ceci est requis pour la finalité du traitement?

Réponse:
L'art. 5 LPD pourrait être considéré comme un motif justificatif pour les mises à jour périodiques et automatiques.

Détails sur les réponses des responsables de la protection des données:
Aucune réponse n'a été faite à ce sujet.

5.4 Profils de personnalité et profilage

Sont-ils créés par une collecte des attributs des profils de personnalité au sens de l'art. 3 lit. d. LPD et, si oui, quelles seraient les conséquences?

Réponse:

Il ne peut pas être exclu que des profils de personnalité soient traités dans le cadre de SWITCH edu-ID. Un traitement des profils de personnalité est justifié selon la loi suisse sur la protection des données au cas par cas avec le consentement de la personne concernée. Les consentements sont obtenus dans chaque cas particulier. Il n'est pas nécessaire de s'appuyer sur une base légale formelle et

supplémentaire. Avec l'entrée en vigueur de la loi suisse révisée sur la protection des données, la notion de «profil de personnalité» est de toute façon très probablement annulée. Le profilage n'est pas exploité dans le cadre de SWITCH edu-ID.

Détails sur les réponses des responsables de la protection des données:
Les délégués à la protection des données LU et FR déclarent que, si des données à caractère personnel sensibles ou particulières sont saisies ou si les données personnelles collectées sont liées à d'autres caractéristiques ou à d'autres informations, de telle sorte qu'il existe des informations sensibles ou même des profils de personnalité, il est indispensable de s'appuyer sur une base légale formelle.

Complément d'informations apporté par SWITCH:
Un «profil de personnalité» est une compilation de données qui permet une évaluation d'aspects essentiels de la personnalité d'une personne physique (art. 3 lit. d LPD). En ce qui concerne un profil de personnalité, il est question d'une compilation d'un très grand volume de données sur la structure de la personnalité, les compétences et activités professionnelles ou même sur les relations et activités extraprofessionnelles qui constituent une image d'ensemble ou une image partielle importante de la personne concernée. Il n'est pas possible de définir de manière générale la notion de profil de personnalité. Quant à la question de savoir si une compilation de plusieurs données d'une certaine personne résulte en un profil de personnalité, le **volume** et le **contenu** des informations relatives à la personne sont déterminants[6].
La notion de «profil de personnalité» est remplacée par **profilage** dans la loi suisse révisée sur la protection des données lors de l'adaptation au RGPD. Le «profilage» est la valorisation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée, notamment pour analyser ou pronostiquer la performance de travail, la situation financière, la santé, le comportement, les préférences, le domicile ou la mobilité (art. 4 lit. f P-LPD). Les notions de «profil de personnalité» et de «profilage» présentent certes des similitudes, mais elles ne sont pas identiques. Tandis que le profil de personnalité est quelque peu statique de manière générale, le profilage décrit un processus dynamique qui est axé sur une certaine finalité.

Le SWITCH edu-ID se compose d'une «identité de base» à laquelle d'autres attributs et affiliations peuvent être ajoutés. Tous les attributs (aussi bien les attributs de l'identité de base que d'autres attributs ajoutés) sont stockés de manière centralisée chez SWITCH. Les attributs contenus dans l'identité de base se trouvent sous le contrôle de l'utilisateur, p. ex. le nom, le prénom et l'adresse e-mail. Comme autres attributs, les utilisateurs peuvent ajouter la date de naissance, un numéro de téléphone ou une adresse et enregistrer des identités comme un ORCID. De plus, SWITCH dispose de la «current affiliation» d'un utilisateur, c'est-à-dire de l'information si un utilisateur est immatriculé/engagé et, si oui, auprès de quelle organisation. De surcroît, SWITCH dispose de l'attribut «affiliation», c'est-à-dire du rôle global (étudiant/collaborateur/membre/personne affiliée) dans lequel un utilisateur est enregistré auprès d'une organisation. Si un utilisateur sort d'une organisation,

[6] Voici des exemples de profils de personnalité: l'enregistrement de transactions de cartes par une entreprise de cartes de crédit dans l'objectif de déterminer si une certaine transaction est inhabituelle pour un certain client; l'enregistrement d'achats par un grand distributeur dans le cadre d'un programme de fidélisation de la clientèle dans l'objectif de se faire une image du comportement de consommation des clients; la compilation de toutes les données d'assurés par une compagnie d'assurance pour pouvoir mieux évaluer quels clients sont les plus intéressants et avec quels produits ils devraient être prospectés.

SWITCH est informée par l'organisation de la sortie et l'ensemble d'attributs «current affiliation» est automatiquement transformé en une «former affiliation», c'est-à-dire l'information de l'organisation dans laquelle un utilisateur a été immatriculé/engagé et jusqu'à quand, et d'éventuels autres attributs comme la branche d'études. La «former affiliation» est stockée chez SWITCH. De plus, il est possible qu'une haute école transmette à SWITCH des «entitlements» tel qu'on les appelle. Ce sont des attributs qui contiennent des informations sur des autorisations spécifiques, p. ex. sous la forme d'une appartenance à un groupe (p. ex. «personne en apprentissage» ou «utilisateur de bibliothèque»). Ces attributs sont requis si un service est uniquement mis à la disposition de personnes qui appartiennent à un tel «groupe» d'ayants droit. La langue de préférence d'une personne est également saisie. Ceci aide les services à afficher l'interface dans la langue souhaitée par l'utilisateur.

SWITCH dispose également des informations auxquelles l'utilisateur a accès, à quel moment et pour quel service (données de connexion). Les informations dont SWITCH ne dispose pas sont celles relatives à la manière dont un service est utilisé. Par exemple, SWITCH sait donc qu'une certaine personne a accédé à un certain moment à un service de bibliothèque, mais SWITCH ne sait pas ce que l'utilisateur a fait dans ce service ou quel livre a été emprunté. De même, SWITCH dispose par exemple de l'information qu'une certaine personne a accédé à un certain moment à Azure (Microsoft Cloud), mais SWITCH ne dispose pas de l'information des documents qui ont été traités avec le service. Ces informations sont uniquement présentées pour les services.

Profil de personnalité en cas de très grand regroupement de données

Un compte edu-ID qui se compose uniquement d'une identité de base avec des attributs minimaux (nom, prénom et adresse e-mail) n'est guère assimilable à un profil de personnalité du fait qu'il ne permet de tirer aucune conclusion sur la personnalité d'une personne. Même un passeport physique ou une carte d'identité physique n'est pas encore assimilable à un profil de personnalité. Plus il y a d'attributs ajoutés à un compte edu-ID, plus il existe un véritable profil de personnalité. Si un compte edu-ID contient par exemple des informations collectées sur une très longue période sur les programmes d'études qu'une certaine personne a achevés ou non et sur quelle période, il est possible d'essayer d'en déduire les caractéristiques principales de la personnalité de la personne X. Il n'est pas possible d'exclure le fait que de telles accumulations d'attributs effectuées sur une très longue période soient qualifiées de profils de personnalité.

Pas de profilage

On ne peut pas parler d'un «profilage» avec le traitement de données edu-ID, pour les raisons suivantes: certes l'historique d'un utilisateur est une collecte de données qui a augmenté au fil du temps et qui est donc «dynamique» – toutefois, les informations ne sont pas collectées dans le but d'analyser les aspects essentiels de la personnalité des utilisateurs ou de prédire leur comportement. La finalité de la collecte de données réside seulement et exclusivement dans l'utilisation des données pour l'administration des hautes écoles ou dans le fait que les utilisateurs peuvent accéder à des services dans le contexte universitaire. En aucun cas l'historique des utilisateurs ne sera analysé pour pouvoir leur envoyer une publicité ciblée pour certains programmes d'études. En conséquence, SWITCH et l'organisation n'effectuent aucun «profilage» lors de l'exploitation de SWITCH edu-ID.

Conséquences

En conséquence du fait que la compilation des données edu-ID peut être qualifiée de profil de personnalité, SWITCH est soumise à des **obligations d'information plus strictes** vis-à-vis des personnes concernées (art. 14 LPD) et le **consentement des personnes concernées est requis au**

cas par cas pour le traitement des données (art. 17 al. 2 lit. c LPD). En outre, le **fichier doit être déclaré au PFPDT** (art. 11a al. 3 lit. a LPD). SWITCH satisfait à toutes ces obligations.

***