Datenschutzbemerkungen zum Bereich E-Learning

Die in den Attributempfehlungen für den Bereich E-Learning definierten Attributen für Geburtsdatum, Geschlecht, Matrikelnummer und Fachsemester unterstützen Hochschulprozesse wie das Ausstellen von Leistungsnachweisen („Scheinen") und zielen damit im Sinne des Datenschutzes explizit auf die Identifikation von Einzelpersonen ab. Da diese Daten in den falschen Händen beispielsweise als Basis für Angriffe wie Impersonation („Identitätsdiebstahl") dienen können, muss ihre Übermittlung an Service Provider in einer AAI besonders sorgfältig gesteuert und kontrolliert werden, um einem Missbrauch vorzubeugen.

Bei den folgenden Ausführungen handelt es sich um Empfehlungen, nicht um rechtlich verbindliche Vorschriften. Es wird ausdrücklich kein Anspruch auf Korrektheit und Vollständigkeit erhoben, sondern vielmehr empfohlen, dass jeder Identity Provider und jeder Service Provider eng mit dem für die jeweilige Einrichtung zuständigen Datenschutzbeauftragten zusammenarbeitet, um die jeweils geltenden Datenschutzgesetze einzuhalten. Insbesondere verbleibt es im Verantwortungsbereich jedes Identity Providers, welche Daten er über welche Benutzer an welche Service Provider übermittelt; der DFN-Verein als Betreiber der DFN-AAI hat hierauf keinen Einfluss und übernimmt keine Verantwortung dafür.

Bemerkungen für Identity Provider

Die im oben genannten Dokument spezifizierten Benutzerattribute werden im Allgemeinen von der Studentenverwaltung der Hochschule, beispielsweise im Rahmen des Immatrikulationsprozesses, erfasst und unter anderem bei der Prüfungsverwaltung genutzt. Bei einer weiteren Verarbeitung dieser Daten, beispielsweise bei ihrer Übernahme in einen Hochschulverzeichnisdienst (LDAP-Server, Identity Management System) mit dem Ziel ihrer Bereitstellung über Shibboleth, ist die Zweckbindung der Daten zu berücksichtigen (vgl. §14 Abs. 1 BDSG und §28 Abs. 2 BDSG). Insbesondere ist im Allgemeinen anzunehmen, dass Bestandsdaten nicht zum Zweck ihrer Weitergabe an externe E-Learning-Anbieter erfasst wurden; somit ist im Allgemeinen die Einwilligung des Betroffenen vor der Weitergabe seiner Daten einzuholen (vgl. §4a Abs. 1 BDSG).

Es wird deshalb dringend empfohlen, einerseits von den in Shibboleth integrierten Schutzmechanismen Gebrauch zu machen und andererseits technische Hilfsmittel zur Information der Betroffenen und der Einholung von Einwilligungen einzusetzen:

- Die Shibboleth Attribute Release Polices (ARPs, v1.3) bzw. Attribut-Filter (v2.0) sollten so voreingestellt werden, dass die in diesem Dokument definierten Attribute nur *selektiv* an einzelne, dem Identity Provider bekannte Service Provider (oder Gruppen von Service Providern) übermittelt werden, mit denen der dienstspezifische Bedarf geklärt wurde.
- Der Benutzer sollte vom Identity Provider darüber informiert werden, welche Daten (Attributnamen und -werte) an den Service Provider, bei dem sich der Benutzer über Shibboleth einloggen möchte, übertragen werden sollen; der Benutzer sollte dabei die Möglichkeit haben, den Vorgang so abzubrechen, dass keine Daten an den Service Provider übermittelt werden. Zur Umsetzung kann beispielsweise die Software uApprove (ehemals ARPViewer) eingesetzt werden, die im Rahmen der SWITCH-AAI implementiert wurde.

Bemerkungen für Service Provider

Für E-Learning-Dienstleister gelten unabhängig vom Shibboleth-Einsatz das Prinzip der Erforderlichkeit (vgl. §28 Abs. 1 Nr. 2 BDSG), das Prinzip der Datensparsamkeit (vgl. §3a BDSG), die Zweckbindung (vgl. §14 Abs. 1 BDSG) und das Prinzip der Erlaubnis durch Einwilligung des Betroffenen (vgl. §4a Abs. 1 BDSG). Beim Abruf von Benutzerdaten mittels einer AAI sollten somit insbesondere folgende Aspekte berücksichtigt werden:

- Ausschlaggebend für den Umfang der abgerufenen Daten ist deren Erforderlichkeit im Learning Management System zur Erbringung der Dienstleistung. Aus der Menge der im oben genannten Dokument spezifizierten Attribute sollten deshalb nur diejenigen vom Identity Provider abgerufen und gegebenenfalls gespeichert werden, für die dies begründet erforderlich ist (Minimalitätsprinzip). Es wird empfohlen, auf die persistente Speicherung personenbezogener Daten seitens des Service Providers so weit wie möglich und sinnvoll zu verzichten.
- Aufgrund des Transparenzgebots (vgl. §4 Abs. 3 BDSG) sollte der Benutzer noch vor seiner Initialregistrierung im System des Service Providers über dessen Betreiber und die Verwendungszwecke der erhobenen Daten informiert werden.

Ein Service Provider muss damit rechnen, dass ein angefordertes Attribut z.B. aufgrund vom Benutzer gesteuerter Datenschutzmechanismen nicht vom Identity Provider geliefert wird. In diesem Fall sollte der Benutzer über die damit verbundenen Diensteinschränkungen informiert werden und beispielsweise über ein Eingabeformular die Möglichkeit erhalten, die fehlenden Daten manuell nachzutragen.

Autor: Dr Wolfgang Hommel, LRZ München