Datenschutzerklärung Shibboleth-Nutzung

1. Verantwortliche Stelle im Sinne der geltenden Datenschutzgesetze ist die Bauhaus-Universität Weimar als Zugangsanbieter.

2. Diese Datenschutzerklärung ist auf der Website der Bauhaus-Universität unter der URL: *http://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/service/shibboleth/datenschutzerklaerung-shibboleth.pdf* jederzeit abrufbar.

3. Nach den datenschutzrechtlichen Bestimmungen der §§ 14, 15 TMG, 95, 97 TKG darf der Zugangsanbieter personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies zum Zweck der Begründung, Durchführung und Abwicklung des Nutzungsverhältnisses betreffend der DFN-AAI und der Angebote der angeschlossenen Service Provider erforderlich ist. Dies erfasst sowohl Bestands- als auch Nutzungsdaten. Bestandsdaten sind beispielsweise Name, Geburtsdatum und Anschrift des Nutzers. Nutzungsdaten sind Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Dienste.

4. Verkehrsdaten werden gemäß den §§ 96, 97, 100 TKG, 15 TMG nur über das Ende der jeweiligen Verbindung hinaus bis zu sechs Monate gespeichert und verarbeitet, soweit diese zum Zweck des Aufbaus weiterer Verbindungen, zur Erkennung und Beseitigung von Störungen und Missbrauch oder zur Entgeltermittlung und Abrechnung der Dienste der DFN-AAI oder der Dienste der Service Provider sowie für die durch andere gesetzliche Vorschriften begründete Zwecke erforderlich sind. Andernfalls werden Verkehrsdaten nach Beendigung der Verbindung unverzüglich gelöscht.

5. Bestandsdaten und Nutzungsdaten werden nach Maßgabe der geltenden gesetzlichen Bestimmungen an die Ermittlungs-, Strafverfolgungs- und Aufsichtsbehörden übermittelt, wenn und soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

6. Beschreibung der Datenverarbeitung in der DFN-AAI

   6.1 Die Infrastruktur zur Authentifizierung und Autorisierung des Deutschen Forschungsnetzes (DFN-AAI) dient dem Zusammenschluss von Hochschulen und sonstigen Bildungseinrichtungen sowie privater Informationsanbieter. Den Teilnehmern dieser Föderation wird auf Grundlage einer technischen Infrastruktur ermöglicht, den lokal in ihren Einrichtungen registrierten Nutzern Ressourcen der gesamten Föderation kontrolliert zur Verfügung zu stellen, ohne dass die Nutzer an allen Einrichtungen einen Nutzeraccount haben.

   6.2 Die technische Realisierung basiert auf Shibboleth, eine vom Internet2-Konsortium entwickelte Software, die eine verteilte Authentifizierung und Autorisierung für Webanwendungen und Webservices ermöglicht.
   Das Konzept von Shibboleth sieht u. A. vor, dass sich ein Nutzer nur einmal pro Browser-Session bei seiner Heimateinrichtung, z. B. der Hochschule, wo dieser immatrikuliert ist, authentifizieren muss, um orts-unabhängig auf Dienste oder lizensierte Inhalte verschiedener Anbieter zugreifen zu können (sog. föderiertes Single-Sign-On). Für die Nutzer ist damit der Zugriff auf die Dienste und Angebote der Teilnehmer der Föderation von jeder Einrichtung aus möglich, wobei diese nach einmaliger Authentifizierung und Autorisierung zur Verfügung stehen.

   6.3 Grundsätzlich werden die Daten eines Nutzers nur an dessen Heimateinrichtung gepflegt, die angebotenen Dienste benötigen nur eigene Nutzerverwaltungen zum Zwecke der Personalisierung und für anwendungsspezifische Daten.

   6.4 An der Bauhaus-Universität Weimar (im Folgenden als Heimateinrichtung bezeichnet) als Zugangsanbieter ist ein Shibboleth Identity Provider an das Identity Management der Heimateinrichtung angeschlossen, der das Single-Sign-On ermöglicht. Die Heimateinrichtung versorgt als Identity-Provider die an der Infrastruktur angeschlossenen Service Provider mit Daten über Authentifizierungs- und Autorisierungsattribute.

6.5 Bei den Service Providern handelt es sich sowohl um öffentliche Stellen als auch um nicht-öffentliche Stellen in Deutschland und im Ausland.

6.6 Wenn ein Nutzer eine über die Föderation zugänglich Ressource anfordert, leitet der Service Provider den Nutzer an einen Dienst (Discovery Service) weiter, wo der Nutzer den Identity Provider seiner Heimateinrichtung auswählt und nachfolgend den Service Provider zurückgeleitet wird, damit dieser die Information über den zur ausgewählten Heimatorganisation gehörigen IdP zwischenspeichern und für weitere Anfragen verwenden kann. Der SP antwortet mit einem an den IdP gerichteten Authentication Request.

6.7 Der Identity Provider an der Heimateinrichtung prüft, ob der Nutzer bereits eine Shibboleth-Session hat, also schon authentifiziert ist. Ist dies nicht der Fall, wird die Authentifizierung eingeleitet, z.B. dem Nutzer ein Formular zur Eingabe von Benutzerkennwort und Passwort angezeigt. Ist der Benutzer authentifziert, wird je eine SAML-Authentifizierungs- und Attribut-Assertion für den Service Provider ausgestellt.

6.8 Der SP prüft nun anhand der Assertions, ob der Benutzer Zugriff hat, und gibt entsprechend die ursprünglich angeforderte Ressource zurück.

7. Die im Rahmen der DFN-AAI übertragenen personenbezogenen Attribute sind:
   - mail: E-Mail-Adresse des Nutzers
   - givenname und sn: Vor- und Nachname,
   - eduPersonPrincipalName: eine ID, die den Nutzer für Transaktionsprozesse in der AAI identifiziert, welche Namensbestandteile enthalten kann,
   - eduPersonAffiliation: eine Beschreibung der Hauptrollen, die man an der Hochschule innehaben kann. z.B. »student« für Studierende, »staff« für Mitarbeiter, »faculty« für Lehrkörper

   Je nach Service Provider können auch weniger oder mehr Attribute übertragen werden. Welche Attribute im konkreten Fall übertragen werden sollen, wird dem Nutzer vor der Übertragung angezeigt, worauf er seine Zustimmung zur Übertragung geben oder verweigern kann.

8. Die Service Provider setzen sogenannte Cookies ein, um damit Nutzungsdaten von den anfragenden Nutzern zu erheben, verarbeiten und nutzen. Der Einsatz dieser Cookies dient dazu, das Angebot nutzerfreundlich und nutzerbezogen sowie effektiv und sicher auszugestalten.

9. Cookies sind kleine Text-Dateien, die von einem Webserver an den Browser des anfragenden Nutzers gesendet und auf die Festplatte dessen Computers gespeichert werden. Diese Informationen dienen dazu, den Nutzer beim nächsten Besuch auf den Websites des Service Providers automatisch wiederzuerkennen und die Navigation zu erleichtern. Cookies erlauben es beispielsweise, eine Webseite den Interessen des Nutzers anzupassen oder die beim Einloggen für die Authentifizierung abgefragten Daten zu speichern, um ein vereinfachtes Einloggen zu ermöglichen.

10. Die Websites der Service Provider können auch ohne Cookies genutzt werden. So kann der Einsatz von Cookies ausgeschlossen werden, indem die Browser-Einstellungen »keine Cookies zulassen« vom Nutzer gewählt wird. Die Ablehnung von Cookies kann aber zu Funktionseinschränkungen des Angebots der Service Provider führen.

11. Wenn Sie weitergehende Fragen zu den Hinweisen zum Datenschutz und zur Verarbeitung Ihrer personenbezogenen Daten haben, können Sie sich direkt an den Datenschutzbeauftragten ihrer Hochschule wenden.

12. Sofern Sie externe Links nutzen, die im Rahmen des Angebots der DFN-AAI angeboten werden, erstreckt sich diese Datenschutzerklärung nicht auf diese Links. Die Service Provider und Zugangsanbieter haben keinen Einfluss auf die Einhaltung der Datenschutz- und Sicherheitsbestimmungen durch andere Anbieter. Informieren Sie sich deshalb auf den Internetseiten der anderen Anbieter auch über die dort bereitgestellten Datenschutzerklärungen.