Datenschutz bei Adobe Connect

1. Betrieb der Server

Die Server werden vom DFN-Verein betrieben und stehen mit hoher Verfügbarkeit und Ausfallsicherheit an den Kernnetzstandorten im Wissenschaftsnetz. Nur vom DFN-Verein autorisierte Mitarbeiter haben zur Erbringung des Dienstes Zugriff auf die Server (Installation, Betrieb, Wartung, Update).

2. Nutzeranmeldung und Nutzerverwaltung

Die Nutzer geben bei der Anmeldung Vornamen, Namen und E-Mail-Adresse an. Auf dem Server wird ein personalisiertes Konto (Account) mit Login-Daten eingerichtet. Das automatisch erstellte Passwort sollte beim ersten Login unter den persönlichen Einstellungen geändert werden.

Auf dem VC-Portal (https://www.vc.dfn.de/webkonferenzen.html) wird der Nutzer auf Folgendes hingewiesen: "Sie stimmen mit Ihrer Registrierung auf dem Adobe Connect Server zu, dass Ihre personenbezogenen Daten Vorname, Nachname und E-Mail-Adresse für alle auf dem Server registrierten Meeting-Veranstalter einsehbar sind." Die Anzeige der registrierten Nutzer ermöglicht es einem Meeting-Veranstalter bei der Erstellung eines Meetings sofort auf die entsprechenden Nutzer-Einträge zu klicken und die Teilnehmer automatisiert durch eine vom Adobe Connect Server versendete Mail zu dem Meeting einzuladen. Dies ist ein Feature von Adobe Connect, was nicht abstellbar oder im Sinne einer Pseudonymisierung einschränkbar ist. Technisch basiert die Liste der registrierten Meeting-Veranstalter auf einem Flash Applet, das nicht modifizierbar ist.

Neue Nutzer, deren Registrierung per Shibboleth/AAI erfolgt, sollten beim ersten Login von ihrem IdP-Betreiber über einen uApprove-Vorgang geleitet werden und damit in Kenntnis gesetzt werden bzw. zustimmen, das personenbezogene Daten (Vorname, Nachname, E-Mail-Adresse) zur Erbringung des Dienstes erforderlich sind und gespeichert werden und dass diese Daten auf dem Server (nur für registrierte Nutzer) einsehbar sind. Für diesen Vorgang muss jedoch der jeweilige IdP-Betreiber sorgen (siehe https://www.aai.dfn.de/dokumentation/identity-provider/konfiguration/uapprove/).

Bei der Registrierung bzw. Authentifizierung per Shibboleth/AAI übermittelt der IdP neben den Angaben Vorname, Nachname und E-Mail-Adresse auch die Gruppenzugehörigkeit / Leistungsbezugsberechtigung des Nutzers (eduPersonAffiliation, eduPersonScopedAffiliation oder eduPersonEntitlement). Der Grund liegt darin, dass nur "Mitarbeiter" einer Einrichtung zum Dienst zulassen werden, jedoch keine Studenten. Bei der Anmeldung über E-Mail wird die Rolle der Person bei Verdacht (durch Recherche oder Nachfrage) händisch überprüft.

Es werden keine registrierten Nutzer automatisch gelöscht. Nutzer, die 2 Jahre inaktiv waren, werden angeschrieben und gebeten, sich einzuloggen. Erfolgt nach der gesetzten Frist kein Login, werden diese Accounts gelöscht.

3. Datenübertragung und Datenverarbeitung

Die Anmeldung am Server sowie die gesamte Verwaltung und auch der Austausch der Daten (Audio, Video, Datenpräsentationen/Whiteboard) erfolgen verschlüsselt über https.

Alle hochgeladenen Dokumente sowie Aufzeichnungen werden unverschlüsselt auf dem Server gespeichert.

Es werden keine Nutzerdaten automatisch gelöscht.

Bei sehr hohem Datenvolumen einzelner Nutzeraccounts von derzeit mehr als 5 GiB (hochgeladene Dokumente und Aufzeichnungen) werden diese Nutzer angeschrieben und gebeten, Daten zu löschen oder ggf. herunter zu laden.

Meetings können aufgezeichnet werden. Die Aufzeichnungen sind eindeutig der Veranstaltung zugeordnet. Es kann nicht anderweitig darauf zugegriffen werden.

Bei der Aufzeichnung von Meetings gibt es weitere Optionen. Grundsätzlich wird alles aufgezeichnet, was alle sehen können (kein privater Chat). Bei der Nachbearbeitung des Streams hat der Veranstalter aber die Möglichkeit, den gesamten Chat und auch die Teilnehmerliste zu entfernen, wenn das gewünscht ist.