Forschungsdatenzentrum
der Bundesagentur für Arbeit
im Institut für Arbeitsmarkt-
und Berufsforschung

FDZ

FDZ-Methodenreport

08/2012
DE

Methodische Aspekte zu Arbeitsmarktdaten

Technische und organisatorische Maßnahmen für den Fernzugriff auf die Mikrodaten des Forschungsdatenzentrums der Bundesagentur für Arbeit

Jörg Heining,
Stefan Bender

Bundesagentur für Arbeit

Technische und organisatorische Maßnahmen für den Fernzugriff auf die Mikrodaten des Forschungsdatenzentrums der Bundesagentur für Arbeit

Jörg Heining, Stefan Bender

Die FDZ-Methodenreporte befassen sich mit den methodischen Aspekten der Daten des FDZ und helfen somit Nutzerinnen und Nutzern bei der Analyse der Daten. Nutzerinnen und Nutzer können hierzu in dieser Reihe zitationsfähig publizieren und stellen sich der öffentlichen Diskussion.

FDZ-Methodenreporte (FDZ method reports) deal with the methodical aspects of FDZ data and thus help users in the analysis of data. In addition, through this series users can publicise their results in a manner which is citable thus presenting them for public discussion.

Inhaltsverzeichnis

Zusammenfassung

Das Forschungsdatenzentrum (FDZ) der Bundesagentur für Arbeit (BA) im Institut für Arbeitsmarkt- und Berufsforschung (IAB) in Nürnberg bietet einen Fernzugriff auf datenschutzrechtlich sensible Mikrodaten an. Datennutzerinnen und -nutzer können von den Forschungsdatenzentren der Statistischen Ämter der Länder an den Standorten Berlin, Bremen, Düsseldorf, Dresden sowie an der Hochschule der Bundesagentur für Arbeit in Mannheim auf die Daten des FDZ zugreifen. Zusätzlich besteht diese Möglichkeit auch am Institute for Social Research (ISR) der University of Michigan in Ann Arbor, MI, USA. Dieser Methodenreport beschreibt die für diesen Fernzugriff notwendigen technischen und organisatorischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben.

Abstract

The Research Data Center (FDZ) of the Federal Employment Agency (BA) at the Institute for Labour Market and Employment Research (IAB) in Nuremberg for the first time provides a remote access to confidential microdata. Data users can access data of the FDZ from the research data center of the Statistischen Ämter der Länder with offices in Berlin, Bremen, Dusseldorf, Dresden and at the University of Applies Labor Studies of the German Federal Employment Agency in Mannheim. Additionally, this possibility also exists at the Institute for Social Research (ISR) of the University of Michigan in Ann Arbor, MI, USA. This report describes the technical and organizational methods necessary for ensuring data confidentiality.

Keywords: Remote Access, Datenschutz

Die diesem Methodenreport zugrundeliegenden Vorhaben wurden mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01UW1002 sowie mit des Mitteln für das Projekt „Data without Boundaries“ im Rahmen des Siebten Framework Programmes (FP7/2007-2013) der Europäischen Union unter der Fördernummer 262608 gefördert.

1 Einleitung

Das Forschungsdatenzentrum (FDZ) der Bundesagentur für Arbeit (BA) im Institut für Arbeitsmarkt- und Berufsforschung (IAB) in Nürnberg bietet einen Fernzugriff auf datenschutzrechtlich sensible Mikrodaten an. Datennutzerinnen und –nutzer können seit Oktober 2011 von den Forschungsdatenzentren der Statistischen Ämter der Länder an den Standorten Berlin, Bremen, Düsseldorf, Dresden sowie an der Hochschule der Bundesagentur für Arbeit in Mannheim auf die Daten des FDZ zugreifen. Zusätzlich besteht diese Möglichkeit auch am Institute for Social Research (ISR) der University of Michigan in Ann Arbor, MI, USA. Die Ausweitung auf weitere Standorte sowohl im europäischen Ausland (im Rahmen des von der Europäischen Union geförderten Data without Boundaries (DwB) Projektes, www.dwbproject.org) als auch in Nordamerika ist geplant.

Um im Rahmen von Gastaufenthalten Zugang zu den Mikrodaten des FDZ zu erhalten, mussten Nutzerinnen und Nutzer in der Vergangenheit nach Nürnberg kommen. Im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) finanzierten und vom Rat für Wirtschafts- und Sozialdaten (RatSWD) begutachteten Projektes „Forschungsdatenzentrum-im-Forschungsdatenzentrum“ (PFiF) wurde die Möglichkeit eines Fernzugriffs implementiert. Die Grundidee ist hierbei, dass Forscherinnen und Forscher über eine sichere Internetverbindung Zugang zu den Daten des FDZ bekommen (so genannter Remote Access), die Daten selbst aber in Nürnberg verbleiben. Nach Abschluss eines Nutzungsvertrages mit dem FDZ können Forscherinnen und Forscher sich an bisher sechs Standorten mit Hilfe eines so genannten Thin Client Rechners auf einem Server im abgeschotteten Netzwerk des FDZ verbinden. Auf diesem Server erfolgt die eigentliche Datenverarbeitung, die Thin Client Rechner dienen somit lediglich zum Verbindungsaufbau. Die Verschlüsselung der Verbindung zwischen Thin Client Rechner und dem Server in Nürnberg erfolgt unter Verwendung des von der Firma Citrix entwickelten Access Gateways.

Der vorliegende Methodenreport beschreibt die technische Umsetzung sowie die ergriffenen organisatorischen und technischen Maßnahmen, die zur Einhaltung der datenschutzrechtlichen Vorgaben für einen derartigen Fernzugriff notwendig sind. Zunächst wird die Grundidee dieses Fernzugriffs dargestellt, bevor auf die formalen Kriterien, d.h. Antragsverfahren und Nutzungsvertrag eingegangen wird. In Abschnitt 4 erfolgt die Beschreibung der technischen Umsetzung, während Abschnitt 5 die technischen und organisatorischen Maßnahmen im Detail beschreibt. Abschnitt 6 schließt mit einem Ausblick auf zukünftige Entwicklungen.

2 Grundidee

Die Grundidee bei der Implementierung dieses Fernzugriffs besteht darin, Zugriff auf die Mikrodaten des FDZ aus den Räumen eines anderen Forschungsdatenzentrums (unterschiedliche Institution und Verortung) zu ermöglichen. Der Datenzugang erfolgt analog zur bisherigen Praxis der Gastaufenthalte im FDZ der BA im IAB. Der einzige Unterschied besteht darin, dass sich der Gastraum, in dem der Forscher vor Tastatur und Bildschirm sitzt, nicht im

FDZ der BA im IAB in Nürnberg, sondern in einem anderen FDZ (Gast-FDZ) befindet. Der Zugriff auf die Daten erfolgt von dedizierten Arbeitsplätzen im Gast-FDZ. Im Gast-FDZ müssen hierfür die gleichen Sicherheitskriterien erfüllt sein wie im FDZ der BA im IAB. Der Zugriff erfolgt über eine sichere Datenleitung. Wichtig ist dabei, dass im Gast-FDZ die Daten weder verarbeitet noch gespeichert werden. Dies geschieht wie bisher auf einem geschützten Server in Nürnberg. Im Gast-FDZ wird lediglich die Verbindung zu den Datenverarbeitungssystemen in Nürnberg hergestellt und die Zutrittskontrolle sichergestellt (siehe Abbildung 1: Grundidee). Antrags- und Vertragsbearbeitung, Nutzerverwaltung, Administration des FDZ Gästenetzes und die Outputkontrolle verbleiben in der Zuständigkeit des FDZ der BA im IAB in Nürnberg.

Hinsichtlich des Betreuungskonzeptes der Standorte gibt es Unterschiede zwischen Deutschland und den USA. In Deutschland übernimmt ein fest definierter und enger Personenkreis von Mitarbeitern am jeweiligen Standort die Betreuung des Datenzugangs. Diese Mitarbeiter erhalten selbst keinen Zugang zu den Daten des FDZ. Sie setzen nur die notwendigen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes durch. Am Standort in Ann Arbor ist derzeit dagegen ein Mitarbeiter des FDZ der BA im IAB vor Ort tätig.

Im Hinblick auf den Anonymisierungsgrad der Daten gibt es keinen Unterschied zwischen einem Gastaufenthalt in Nürnberg oder an einem der externen Standorte. Sowohl in Nürnberg als auch an den Standorten der FDZ-StaLä und der HdBA können berechtigte Datennutzer auf schwach anonymisierte Daten zugreifen. Anders dagegen am Standort Ann Arbor. Hier werden die Datensätze durch die Mitarbeiter des FDZ anonymisiert, sodass im Rahmen dieses Fernzugriffs keine schwach anonymisierten Daten in die USA übermittelt werden.

Ein zentraler Bestandteil im Rahmen der Gewährleistung des Datenschutzes im FDZ der BA im IAB besteht darin, dass nur absolut anonymisierte Ergebnisse und Dateien den abgeschotteten Bereich des FDZ Gästenetzes verlassen. Die Mitarbeiter des FDZ der BA im IAB stellen durch Prüfung der vom Nutzer erzeugten Ergebnisdateien sicher, dass keine Einzelangaben (z.B. Betriebe, Haushalte, Individuen) identifiziert werden können. Diese Grundsätze gelten auch für Datennutzungen an den externen Standorten. Auch bei einer Datennutzung außerhalb des Standortes Nürnberg wird dem Datennutzer durch das FDZ der BA im IAB nur absolut anonymer Output übermittelt. Eine selbständige Entnahme von Daten- oder Ergebnisdateien durch den Nutzer am externen Standort ist durch die technische Umsetzung (siehe Abschnitt 4 und 5) nicht möglich.

Neben den mit externen Datennutzern geschlossenen Nutzungsverträgen regeln vertragliche Vereinbarungen zwischen dem FDZ der BA mit den Gast-FDZ bzw. den Institutionen der Gast-FDZ die Rechte und Pflichten dieser Außenstellen.

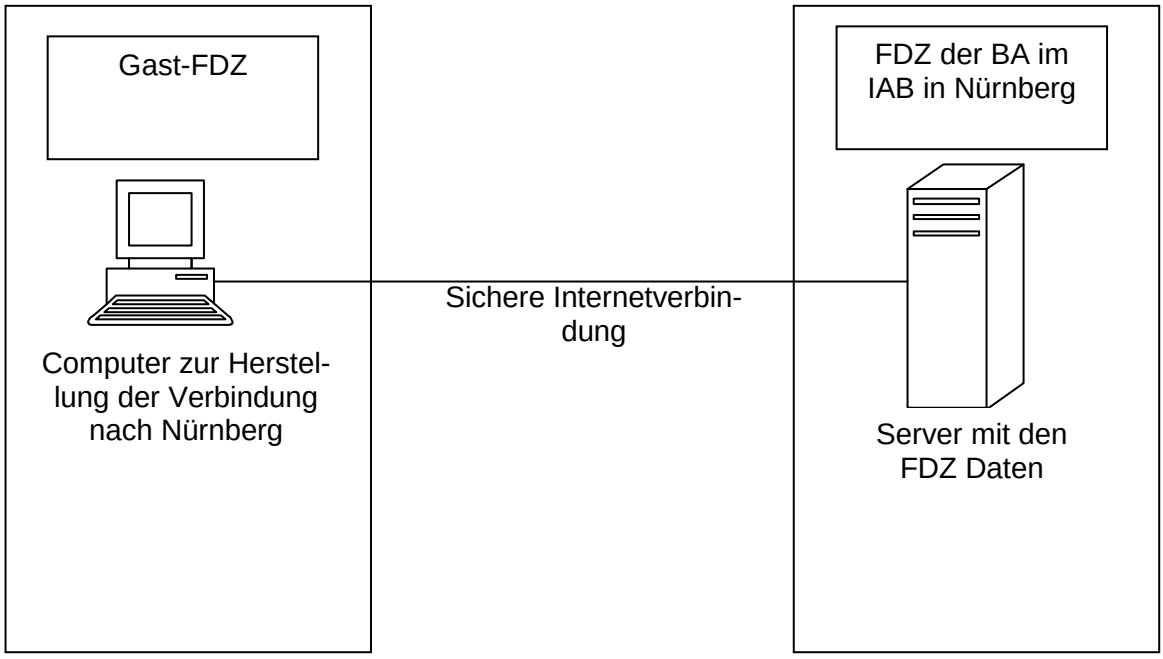

Abbildung 1: Grundidee

3 Antrag auf Datenzugang und Nutzungsvertrag

Beim FDZ der BA im IAB stellen alle externen Forscher einen Antrag auf Datenzugang nach § 75 des zehnten Sozialgesetzbuches (SGB X). Dieser wird nach Prüfung durch die Mitarbeiter des FDZ der BA im IAB in Nürnberg an das Justitiariat des IAB gegeben und von dort aus an das Bundesministerium für Arbeit und Soziales (BMAS) weitergeleitet. Nach der Genehmigung des Forschungsprojektes durch das BMAS schließt das FDZ der BA im IAB mit der Institution des Nutzers einen Vertrag auf Datenzugang, in dem sich der Nutzer verpflichtet, die dort festgehaltenen Regelungen zum Datenschutz zu beachten und bei Vertragsbruch die im Nutzungsvertrag bzw. deutschen Recht vorgesehenen Konsequenzen zu tragen. Ferner erfolgt eine gesonderte Verpflichtung aller Nutzer, die nicht in einem Beschäftigungsverhältnis zum öffentlichen Dienst stehen, auf die gesetzlichen Regelungen zum deutschen Datenschutz.

Neben Projekttitel, einer Projektbeschreibung, der Laufzeit und des Datenbedarfs legt der Nutzungsvertrag explizit Verhaltensregeln beim Arbeiten mit den Daten des IAB/des FDZ der BA im IAB fest. Diese Verhaltensregeln gelten an allen der oben genannten Standorte.

Die zwischen dem FDZ und dem externen Datennutzer geschlossenen Verträge sind „standortunabhängig“ und erlauben die Datennutzung sowohl in Nürnberg als auch an einem der oben genannten Standorte. Es ist jedoch zu beachten, dass für die Datennutzung in Ann Arbor neben einem geprüften Antrag, der Genehmigung durch das BMAS und dem Vorliegen eines gültigen Nutzungsvertrages weitere Zugangsvoraussetzungen, wie z.B. die Genehmigung des Projektes durch ein Institutional Review Board (dies entspricht einer Ethikkommission) gelten. Dies ist der in den USA geltenden rechtlichen Praxis hinsichtlich des

Zugangs bzw. der Verwendung von Mikrodaten auf Personenebene geschuldet. Erfüllt ein Datennutzer diese Voraussetzungen nicht, ist ein Datenzugang in den USA nicht möglich. Ein Datenzugang an einem der deutschen Standorte oder in Nürnberg ist davon aber nicht betroffen.

4 Technische Umsetzung

4.1 Grundkonzept

Die technische Umsetzung des Fernzugriffs auf die Daten des FDZ erfolgt durch so genannte Thin Client Rechner (siehe unten). An jedem der oben genannten Standorte steht mindestens eines dieser Geräte, die es dem Nutzer an einem externen Standort erlauben, sich über eine sichere Internetverbindung in das FDZ Gästenetz in Nürnberg einzuwählen. Die Datenverarbeitung erfolgt nicht auf den Thin Client Rechner am externen Standort, sondern auf einem Server im abgeschotteten FDZ Gästenetz.

Die Thin Client Rechner befinden sich an allen Standorten hinter der Firewall des jeweiligen Standortes. Ebenso sind die Server in Nürnberg durch eine entsprechende Firewall abgesichert.

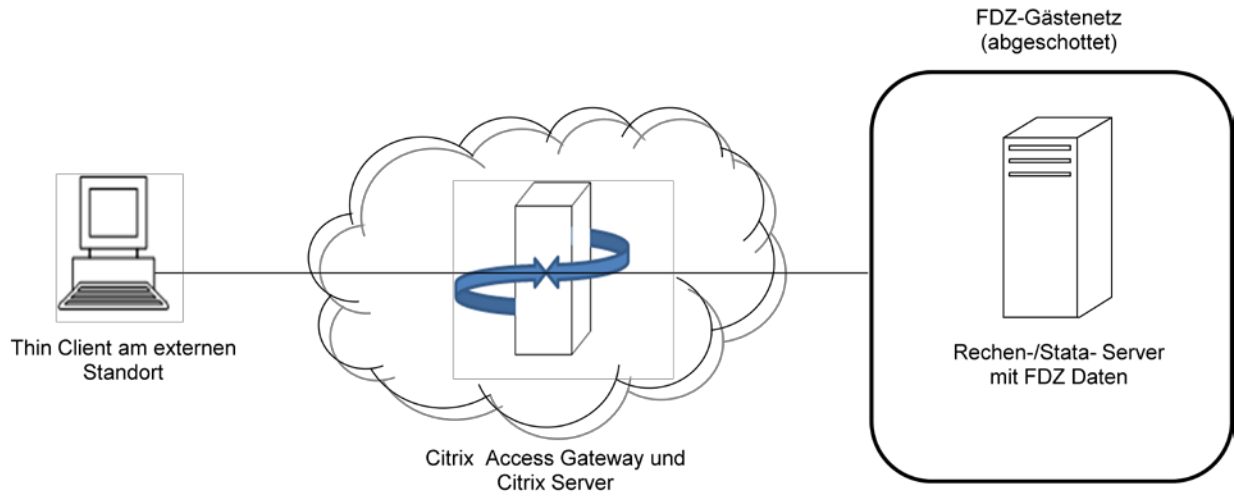

Abbildung 2: Technische Umsetz des Fernzugriffs auf Daten des FDZ (sehr vereinfachte und schematische Darstellung)

4.2 Thin Client

Unter einem Thin Client Computer versteht man einen Rechner, der im Gegensatz zu herkömmlichen Rechnern mit weniger Hardware(-leistung) ausgestattet ist. Ein Thin-Client stellt lediglich die Benutzerschnittstelle zu einem Server dar. Die eigentliche Kommunikation, Datenverarbeitung und die Speicherung der Daten erfolgen auf dem Server.

Die Thin Clients dieser Lösung verfügen über keinerlei Anschlussmöglichkeiten für Wechselmedien (USB Stick, externe Festplatte, usw.) oder externe Peripheriegeräte (Drucker, externe optische Laufwerke usw.). Einem externen Datennutzer ist es daher nicht möglich, Software oder Dateien auf dem Thin Client aufzuspielen oder zu entnehmen.

Darüber hinaus ist die für einen externen Datennutzer verfügbare Software auf dem Thin Client Rechner stark limitiert. Dem Datennutzer steht lediglich der Windows Internet Explorer zur Verfügung, der für den Verbindungsaufbau zum Server nach Nürnberg benötigt wird. Nach dem Öffnen des Internet Explorers gelangt der Nutzer auf eine voreingestellte Seite, von der aus der Verbindungsaufbau erfolgt. Der Datennutzer kann sich zu keinem Zeitpunkt auf eine andere Internetseite verbinden oder die voreingestellte Seite ändern. Weitere Software steht dem Benutzer auf dem Thin Client nicht zur Verfügung.

Die Thin Client Rechner wurden grundsätzlich so konfiguriert, dass solange keine Verbindung zum Server besteht, der Datennutzer am Thin Client nur den Windows Internet Explorer öffnen kann. Andere Funktionalitäten sind nicht vorhanden bzw. können vom Nutzer zwar aufgerufen werden, allerdings bleiben durchgeführte Änderungen aber wirkungslos.

4.3 Citrix Access Gateway und Citrix Server

Der Verbindungsaufbau zwischen Thin Client Rechner am externen Standort und einem Server im FDZ Gästenetz erfolgt über die Access Gateway Software und einem dazugehörigen (und durch die BA beschafften) Server der Firma Citrix. Hiermit wird eine verschlüsselte Verbindung zwischen dem Thin Client und dem Server im FDZ Gästenetz über ein öffentliches Netzwerk aufgebaut, wodurch eine zuverlässige Datenübermittlung und ein sicherer Fernzugriff möglich sind. Kommunikationsinhalte zwischen dem FDZ Server und dem Thin Client werden dabei verschlüsselt und die beteiligten Kommunikationspartner, FDZ Server und Thin Client, müssen sich gegenseitig authentifizieren. Die so etablierte (temporäre) Verbindung erfüllt den höchsten Sicherheitsstandard. Somit ist die Kommunikation zwischen Server und Thin Client für Dritte, d.h. einen potentiellen Angreifer auf die Daten, nicht lesbar. Citrix wird weltweit eingesetzt und wird beispielsweise von anderen FDZ im Ausland (z.B. in den Niederlanden oder Dänemark), aber auch von Banken verwendet.

Zum Aufbau einer sicheren Verbindung vom Thin Client Rechner zum Server im FDZ Gästenetz startet der Datennutzer am externen Standort den Windows Internet Explorer am Thin Client. Die voreingestellte Internetadresse führt den Nutzer zur Citrix Eingabemaske, in der der personalisierte Benutzername und das Kennwort für das Projekt vom Nutzer einzugeben sind.

Der Verbindungsaufbau ist zudem durch ein weiteres Kennwort gesichert. Dieses ist nur dem vor Ort betreuenden Mitarbeiter bekannt und wird nicht an den externen Datennutzer weitergegeben (siehe Abschnitt 4.2). Das Verbindungspasswort wird in regelmäßigen Abständen geändert.

4.4 FDZ Gästenetz

Die tatsächliche Datenverarbeitung erfolgt im Gästenetz des FDZ der BA im IAB. Das FDZ Gästenetz ist ein abgeschottetes Netzwerk bestehend aus mehreren Servern. Bis auf einige, für Wartungsarbeiten des BA IT-Systemhauses freigeschaltete Zugänge (Ports) besteht keine Verbindung zwischen dem Intranet der BA oder der Außenwelt (Internet) und dem FDZ Gästenetz. Ein Zugriff auf das FDZ Gästenetz von außerhalb ist nur über die Thin Clients an den oben genannten Standorten möglich. Diese müssen sich bei Einwahl in das FDZ Gästenetzwerk authentifizieren.

Das Gästenetz wurde von den Experten des BA IT-Systemhauses und dem Geschäftsbereich IT und Informationsmanagement des IAB eingerichtet. Es erfüllt die geltenden IT Sicherheitsstandards der BA. Die gesetzlichen Vorgaben nach § 78a SGB X bzw. der Anlage zu § 78a SGB X zur Zugriffs,- Eingabe-, Weitergabekontrolle usw. sind im FDZ Gästenetz erfüllt (siehe Abschnitt 4).

5 Organisatorische und technische Maßnahmen

Nach der Beschreibung der Grundidee und der technischen Umsetzung dieses Fernzugriffs soll nun die organisatorische Umsetzung erläutert werden. Die Darstellung orientiert sich dabei an den in Anlage zu § 78a SGB X geforderten technischen und organisatorischen Maßnahmen für den Zugang zu personenbezogenen Daten.

5.1 Zutrittskontrolle

Wie oben ausgeführt erfolgt die eigentliche Datenverarbeitung auf den Server des FDZ Gästenetzes. Auf diesen Servern sind die Daten auch gespeichert. Die Server sind in den Rechenzentren der BA untergebracht. Hier gelten die höchsten Sicherheitsstandards im Hinblick auf bauliche und organisatorische Maßnahmen, um den Serverraum vor dem Zutritt Unberechtigter zu schützen.

Das FDZ der BA übermittelt den externen Standorten in Deutschland in regelmäßigen Abstand Namenslisten der Datennutzer, welche einen gültigen Nutzungsvertrag zur Durchführung von Gastaufenthalte mit FDZ der BA im IAB geschlossen haben. Dabei muss ein unterzeichneter Nutzungsvertrag des FDZ vorliegen, der Datenzugang im Rahmen von Gastaufenthalten an einem externen Standort explizit berücksichtigt wird.

Zur Durchführung eines Gastaufenthalts vereinbart der Datennutzer mit den zuständigen Mitarbeitern vor Ort einen Termin. Zum jeweiligen Termin wird die Identität des Datennutzers von den Mitarbeitern der FDZ-StaLä oder der HdBA anhand eines gültigen Ausweisdokumentes (Reisepass oder Personalausweis) überprüft und mit der vom FDZ übermittelten Namensliste abgeglichen.

Am Standort Ann Arbor erhält ein Datennutzer ebenso nur nach vorheriger Terminvereinbarung mit dem Mitarbeiter des FDZ der BA im IAB vor Ort Zugang zu den Thin Client Rechner. Der Mitarbeiter des FDZ der BA im IAB überprüft die Identität des Datennutzers anhand ei-

nes gültigen Ausweisdokumentes. Die Übermittlung von Namenslisten der berechtigen Datennutzer an den Mitarbeiter in Ann Arbor ist nicht notwendig, da dieser Zugriff auf die Nutzerdatenbank des FDZ der BA im IAB hat, in der diese Information hinterlegt ist.

Für alle Standorte gilt, dass externe Datennutzern nur zu bestimmten Öffnungszeiten Zutritt zu den Thin Client Rechnern erhalten können. An jedem Standort ist der Zutritt, z.B. durch eine Pforte, zusätzlich gesichert. Die Räume mit den Thin Client Rechnern werden stets verschlossen gehalten und werden nur für die Datennutzung durch einen zugelassenen Nutzer geöffnet. In diesen Räumen sind die Thin Client Rechner zusätzlich mit Kensington Schlösser gegen Diebstahl gesichert. Grundsätzlich gilt, dass die Nutzung der Thin Client Rechner durch den Datennutzer ausschließlich in Anwesenheit der für den Standort verantwortlichen Betreuer erfolgt.

5.2 Zugangskontrolle

Unabhängig vom Standort wird für alle Datennutzer mit einem gültigen Datennutzungsvertrag, der zum Gastaufenthalt berechtigt, ein Projektverzeichnis auf den Servern im FDZ Gästenetz eingerichtet. In diesem Verzeichnis werden die vertraglich vereinbarten Daten abgelegt. Der Datennutzer kann auf dieses Projektverzeichnis nur zugreifen, wenn er sich mit seinem Benutzernamen und seinem persönlichen Passwort am FDZ Gästenetz anmeldet. Dem Datennutzer ist es nicht möglich auf andere Projekt- oder Datenverzeichnisse zuzugreifen.

Sowohl Benutzername als auch Passwort sind projekt- und personenspezifisch und nur dem Datennutzer bekannt. Dem Datennutzer ist die Weitergabe von Benutzername und Passwort vertraglich strengstens untersagt. Benutzerkennung wie auch Passwort sind nur für die vertraglich vereinbarte Projektdauer aktiviert. Nach Projektende ist kein Zugang zum Projektverzeichnis für den Nutzer mehr möglich.

Bei den externen Standorten ist der Zugang zu den Datenverarbeitungssystemen, d.h. den Servern im FDZ Gästenetz, zusätzlich abgesichert. Zum einen ist den Mitarbeitern an den externen Standorten weder der Benutzername noch das Passwort des Datennutzers bekannt. Die Zugangsdaten werden dem Datennutzer nach Feststellung der Identität durch die Betreuer der Standorte vom FDZ der BA telefonisch übermittelt.

Darüber hinaus ist die Verbindung vom Thin Client Rechner zum Server in Nürnberg durch ein zusätzliches Passwort geschützt. Dieses Passwort ist nur den Standortbetreuern vor Ort bekannt, jedoch nicht dem Nutzer. Das Verbindungspasswort wird in regelmäßigen Abständen geändert. Bei Inaktivität des Thin Client Rechners wird die Verbindung zum Server in Nürnberg getrennt und kann nur durch erneute Eingabe des Verbindungspasswortes wieder aktiviert werden.

Es liegt somit eine doppelte Sicherung im Rahmen dieses Fernzugriffs vor: Zum einen durch projekt- und personenspezifische Benutzerkennungen und Passwörter, zum anderen auf-

grund des Verbindungspasswortes. Beide Elemente sind zur Datennutzung an einem der externen Standorte zwingend notwendig.

5.3 Zugriffskontrolle

Siehe Abschnitt 4.2. Die Server des FDZ Gästenetz in Nürnberg sind nicht mit dem Internet verbunden. Mit Ausnahme der speziell konfigurierten Thin Client Rechner und unter Benutzung des Citrix Access Gateways sowie des Citrix Servers ist kein Zugriff über das Internet auf diese Server möglich.

5.4 Weitergabekontrolle

Die Thin Client Rechner erlauben keinen Anschluss von Wechselmedien oder Peripheriegeräten. Daher ist es dem Datennutzer am Standort nicht möglich über die Thin Clients Dateiabzüge oder Auszüge der Daten zu entnehmen. Mittels der Citrix Access Gateway Lösung wird eine sichere Verbindung vom Thin Client zum Server im FDZ Gästenetz in Nürnberg aufgebaut, die für Dritte nicht einsehbar ist. Insofern können auch auf diesem Wege keine Daten entnommen und weitergegeben werden.

Der Datennutzer erhält lediglich von Mitarbeitern des FDZ der BA im IAB geprüfte Protokoll- und Ergebnisdateien die absolut anonym sind. Die Identifikation eines Einzelfalls ist mit diesen Protokoll- und Ergebnisdateien somit nicht möglich. Die hierbei vom FDZ der BA angewandten Kriterien sind in Hochfellner et al. (2012) beschrieben.

Zusätzlich wird von den Standortbetreuern sichergestellt, dass Datennutzer am externen Standort keinerlei Abschriften vom Bildschirm der Thin Client Rechner machen. Den Datennutzern ist die Kommunikation mit Externen in den Räumlichkeiten der Thin Client Rechner untersagt. Gleiches gilt für die Verwendung von Mobiltelefonen, Kameras, tragbaren Rechnern usw. Die Einhaltung dieser Vorschriften wird ebenfalls von den Standortbetreuern überwacht und sichergestellt. Es gelten somit die gleichen Regeln wie am Standort Nürnberg.

5.5 Eingabekontrolle

Jeglicher Zugriff auf das FDZ Gästenetz wird protokolliert. Sollten Unregelmäßigkeiten eines Nutzers festgestellt werden, so kann die Zugriffsberechtigung sofort entzogen werden und die vertraglich festgesetzten Strafen werden umgesetzt.

5.6 Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Sozialdaten

Beantragt ein Datennutzer Zugang zu mehreren, im FDZ der BA angebotenen Datensätzen für ein Forschungsprojekt, so wird im FDZ Gästenetz für jedes Datenprodukt ein gesondertes Verzeichnis angelegt. Der Datennutzer kann zwar auf jedes dieser zu seinem Projekt gehörigen Verzeichnisse zugreifen, es ist ihm jedoch nicht möglich Datensätze, auch nicht in Auszügen, zwischen den Verzeichnissen zu verschieben. Somit wird zum einen unterbunden, dass es durch das Zusammenspielen verschiedener Datenprodukte zu einer Erhöhung des Reidentifikationsrisikos für einen Einzelfall kommt. Zum anderen ist durch diese Maßnahme

die getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Sozialdaten gewährleistet.

6 Erweiterungen der Standorte

Das FDZ der BA plant in naher Zukunft zunächst die Ausweitung der externen Standorte in den USA. Nach Vorbild der bisherigen Standorte soll Zugang zu den Daten des FDZ in Zukunft auch an der Cornell University in Ithaca, NY und der University of California at Berkeley angeboten werden. In einem weiteren Schritt soll im Rahmen des Data without Boundaries Projektes auch auf europäischer Ebene zusätzliche Standorte eingerichtet werden.

Auch an den beiden neuen Standorten in den USA gelten die gleichen Regeln und Voraussetzung zur Beantragung des Datenzugangs. Jedoch müssen die Datennutzer wie in an der University of Michigan ggf. zusätzliche Anforderungen erfüllen, um die in den USA geltenden datenschutzrechtlichen Regelungen zu berücksichtigen.

Hinsichtlich der technischen Umsetzung bestehen keine Unterschiede zu den bisherigen Standorten. Im Gegensatz zum Standort in Ann Arbor werden an der University of California und an der Cornell University keine Mitarbeiter des FDZ der BA im IAB dauerhaft vor Ort sein. Die Zutrittskontrolle und die Feststellung der Identität der Datennutzer werden an diesen Standorten durch Beschäftigte der jeweiligen Gast-FDZ erfolgen. Diese FDZ Mitarbeiter sollen, wie Mitarbeiter des öffentlichen Dienstes in Deutschland, auf die Regelungen des Datenschutzes nach deutschem Recht verpflichtet werden. Ferner werden die verantwortlichen FDZ Mitarbeiter in Berkeley und Cornell vom FDZ der BA im IAB hinsichtlich der datenschutzrechtlichen Regelungen in Deutschland sowie der Abläufe im FDZ geschult. Darüber hinaus werden Mitarbeiter des FDZ der BA im IAB in regelmäßigen Abständen die beiden Standorte besuchen und die Einhaltung aller technischen und organisatorischen Maßnahmen überprüfen und sicherstellen.

Wie an den externen Standorten in Deutschland wird das FDZ der BA im IAB in Nürnberg den verantwortlichen Personen vor Ort Namenslisten der berechtigen Datennutzer übermitteln. Somit wird sichergestellt, dass auch in Berkeley und Cornell nur berechtigte Datennutzer Zugang zu den Thin Client Rechnern erhalten. Ansonsten werden technische Umsetzung, sowie die organisatorischen und technischen Maßnahmen zur Gewährleistung des Datenschutzes identisch zu den jetzigen externen Standorten sein.

Auch an den angedachten europäischen Standorten wird die technische und organisatorische Umsetzung im Wesentlichen den Maßnahmen an den derzeitigen Standorten entsprechen. Inwieweit Zusatzanforderungen hinsichtlich des Antragsverfahrens für den Datenzugang oder an das Betreuungskonzepten vor Ort gestellt werden, ist im Moment noch nicht absehbar.

Literatur

Bender, Stefan; Heining, Jörg (2011): The Research-Data-Centre in Research-Data-Centre approach: A first step towards decentralised international data sharing. In: IASSIST Quarterly, Vol. 35, No. 3, S. 10-16.

Hochfellner, Daniela; Müller, Dana; Schmucker, Alexandra; Roß, Elisabeth (2012): Datenschutz am Forschungsdatenzentrum. (FDZ Methodenreport, 06/2012), Nürnberg, 27 S.

Impressum

FDZ-Methodenreport 08/2012

Herausgeber
Forschungsdatenzentrum (FDZ)
der Bundesagentur für Arbeit
im Institut für Arbeitsmarkt- und Berufsforschung
Regensburger Str. 104
90478 Nürnberg

Redaktion
Stefan Bender, Dagmar Theune

Technische Herstellung
Dagmar Theune

Bezugsmöglichkeit
http://doku.iab.de/fdz/reporte/2012/MR_08-12.pdf

Internet
http://fdz.iab.de/

Rückfragen zum Inhalt an:
Dr. Jörg Heining,
Forschungsdatenzentrum (FDZ)
Regensburger Str. 104,
90478 Nürnberg
Tel: 0911 / 179-5392
E-Mail: Joerg.Heining@iab.de