

**Vorlage für den Workshop**  
**„Virtuelle Arbeitsumgebung für sozioökonomische Forschung und Bericht-  
erstattung: Rechtliche Aspekte der Nutzung von Forschungsdaten“**  
**am 05. November 2010 im Studentenwerk Göttingen, Clubraum 4, Platz  
der Göttinger Sieben 4 (Campus), 37073 Göttingen**

### **Gliederung**

1. Begriffsklärungen (aus der Expertise)
2. Grundzüge kollaborativer Datennutzung in einer virtuellen Arbeitsumgebung: Kurzfassung des Anwendungsbeispiels aus der Expertise unter dem Gesichtspunkt: Wie ändern sich Arbeitsabläufe bei der Datennutzung?
3. Mögliche Lösungen für Datensicherheit (aus der Expertise)
4. Fragen an Forschungsdateneinrichtungen

### **1. Begriffsklärungen**

In der folgenden Zusammenfassung wird von Originaldatensätzen und Arbeitsdatensätzen gesprochen. Mit Originaldaten sind zum derzeitigen Stand der Diskussion vor allem Scientific Use Files (SUF) von den Daten haltenden Instituten gemeint. Alle aus den SUFs extrahierten und bereits bearbeiteten Datensätze werden Arbeitsdatensätze genannt.

In der virtuellen Arbeitsumgebung werden über eine graphische Nutzerschnittstelle eine Reihe von Werkzeugen, die auf technische Lösungen im darunter liegenden Systemkern zugreifen, zur Verfügung gestellt. Die Funktionen erledigen folgende Aufgaben:

- Datenverwaltung – Operationen ähnlich denen eines Dateisystems, Versionsverwaltung, logische Verknüpfungen, Festlegung von Nutzungsrechten und -zeiträumen, Suchfunktionen
- Datenbearbeitung – hauptsächlich Editieren von Syntaxdateien
- Datenvergleich – Werkzeuge zum Vergleich zweier Syntaxdateien oder Syntaxdateiversionen
- Datenverarbeitung – Durchführen von statistischen Berechnungen mit R
- Datenanbieterzugriff – Zugang zu Originaldaten von FDZ, Fernrechnen und Ablage von Daten zur langfristigen Archivierung
- Konfiguration – System-, installations- und nutzerspezifische Einstellungen
- Verwaltung – Verwaltung von Benutzergruppen, Rollen und globalen Rechten

- Kollaboration – Werkzeuge zur Zusammenarbeit der Forscher/innen
- Publikation – Veröffentlichung von Forschungsergebnissen im Forschungsverbund sowie auf Webseiten

## **2. Grundzüge kollaborativer Datennutzung in einer virtuellen Arbeitsumgebung: Beispielhafte Zusammenfassung in der Anwendung: Wie ändern sich Arbeitsabläufe bei der Datennutzung?**

Grundsätzlich werden Scientific Use Files, Zwischenergebnis-Arbeitsdatensätze aus einer vorhergehenden Onsite- Nutzung, oder andere Arbeitsdatensätze in der virtuellen Arbeitsumgebung und nicht wie bisher auf jeder Workstation der Verbundmitarbeitenden, abgelegt. Dazu meldet sich der/die Einzelwissenschaftler/in an der virtuellen Arbeitsumgebung mit einem persönlichen Zertifikat an<sup>1</sup>. Die virtuelle Arbeitsumgebung stattet den/die Wissenschaftler/in, in Form der Autorisierung, mit allen ihm/ihr zur Verfügung stehenden Berechtigungen zur Nutzung der virtuellen Arbeitsumgebung aus. Dies geschieht für den/die Wissenschaftler/in völlig transparent.

Mit Hilfe der Datenverwaltungswerkzeuge werden die SUFs oder Arbeitsdaten abgelegt. Dabei werden automatisch das Dateiformat sowie relevante technische Informationen zu den Daten bestimmt und zur Verifikation angezeigt, welche gegebenenfalls korrigiert werden können. Im gleichen Schritt sind fachliche Metadaten, wie die Herkunft, der fachliche Inhalt und der Verwendungskontext der Daten, in einer dafür vorgesehenen Eingabemaske einzugeben. Im Zusammenhang mit der Herkunft der Daten wird ein möglicher automatischer Löszeitpunkt definiert, um die Anforderungen des bereitstellenden FDZ bezüglich der maximalen Aufbewahrungsdauer zu erfüllen. Des Weiteren können die Zugriffsberechtigungen festgelegt werden. Als Standard wird der/die Wissenschaftler/in der auf ihre Person eingeschränkte Einzelzugriff vorgeschlagen, welcher durch weitere Berechtigungen auf der Basis weiterer einzelner Personen oder ganzer Arbeitsgruppen bzw. Rollen erweitert werden kann. Für jede zusätzliche Berechtigung kann der Zugriffsmodus spezifiziert werden: Nur-Lesen, Lesen und Schreiben, Vollzugriff inkl. Löschen. Zusätzlich werden mögliche dedizierte Speicherorte/Speicheranbieter der virtuellen Arbeitsumgebung angeboten, die der/die Wissenschaftler/in bei Bedarf auswählen kann.

Hat ein Mitglied der virtuellen Arbeitsumgebung nicht selbst den SUF oder Arbeitsdaten abgelegt kann sie oder er, bei entsprechender Berechtigung, den SUF oder Arbeitsdatensätze aus der virtuellen Arbeitsumgebung auf die eigene Workstation downloaden.

Im Anschluss an die Ablage oder den Download der SUFs oder Arbeitsdaten werden Syntaxdateien, wie bisher, mit dem lokalen Editor hergestellt und auf der Workstation lokal mit SPSS, Stata oder SAS bearbeitet. Im Rahmen der Erstellung der Syntaxdaten werden Kommentierungsvorgaben als integrier-

---

<sup>1</sup> Die Erläuterung dieser Zertifikate (PKI) findet sich unter Punkt 3

te fachliche Metadaten in der Syntax hinterlegt. Sollen die Daten mit R verarbeitet werden, wird die Syntax in der virtuellen Arbeitsumgebung erstellt (oder abgelegt), bearbeitet und mit den entsprechenden Datenverarbeitungswerkzeugen direkt in der virtuellen Arbeitsumgebung gestartet. Dabei kann eine Emailadresse hinterlegt werden, an die die virtuelle Arbeitsumgebung Informationen zum Status des Datenverarbeitungsauftrags senden kann.

Die final (lokal) erstellte SPSS-, Stata-, oder SAS-Syntax wird mit Hilfe der Datenverarbeitungswerkzeuge in die virtuelle Arbeitsumgebung abgelegt. Dabei wird der/die Wissenschaftler/in um Bestätigung bzw. Korrektur der Informationen zur Verknüpfung der Syntaxdateien mit bereits abgelegten Forschungsdaten gebeten. Letzteres ist insbesondere dann notwendig, wenn Forschungsdaten und Syntaxdateien getrennt gespeichert werden.

Für die Zusammenarbeit mit Kolleginnen und Kollegen aus dem Forschungsverbund, und damit Nutzer/innen der virtuellen Arbeitsumgebung, können nun die Metadaten der Arbeits- und Syntaxdateien durchsucht werden. Diese Möglichkeit kann vor allem auch dann genutzt werden, wenn zusätzliche Funktionen in die Syntax eingebaut werden sollen und diese bereits durch Kolleginnen oder Kollegen implementiert wurden. Die virtuelle Arbeitsumgebung bietet dementsprechend die Suchbarkeit relevanter Syntaxdateien an.

Zusammengefasst legen nach Projektstart die einzelnen Wissenschaftler/innen, soweit vorhanden und möglich, ihre Forschungsdaten, die dazugehörigen Metadaten sowie die Syntaxdaten in der virtuellen Arbeitsumgebung ab. Dazu werden durch die Projektkoordination eine Struktur in der virtuellen Arbeitsumgebung bzw. Vorgaben zur Standardisierung definiert, um die Ablage der Daten möglichst homogen zu gestalten. Durch Setzen von Zugriffsberechtigungen können SUFs allen berechtigten Wissenschaftlern/innen zentral bereitgestellt werden.

Der Forschungsverbund betreibt mittels der Datenbearbeitungswerkzeuge die Entwicklung von Syntaxdateien gemeinsam und erzielt bessere Ergebnisse als bei rein individuellem Arbeiten. Darüber hinaus besteht mit den Datenverwaltungswerkzeugen die Möglichkeit vorhandene freigegebene Syntaxdateien zu durchsuchen und auf relevantes Material zurückzugreifen. Hierdurch wird der Forschungsprozess für den Verbund optimiert.

Auf Basis der mittels der Datenverwaltungswerkzeuge erfassten Metadaten durchsuchen die Arbeitsgruppen des Verbundes vorhandene Forschungsdaten. Damit können Sie auf eine breitere relevante Datenbasis zurückgreifen, die ohne einen strukturierten Überblick in vergleichbarer Form nicht erzielt werden kann.

Der Forschungsverbund entwickelt im Laufe des Projekts komplexe Zusammenhänge, die im Intranet mittels der vorhandenen Kollaborationswerkzeuge dokumentiert werden. Die damit verbundene Historie zu allen Änderungen unterstützt die Forschenden im Hinblick auf die Transparenz des gemeinsamen Forschungsprozesses und der gemeinsamen Entwicklung wissenschaftlich wertvoller Erkenntnisse.

Zum Abschluss von Projektphasen bzw. Projekten werden die erarbeiteten Ergebnisdaten sowie die verwendete Syntax mit Hilfe der Datenverwaltungswerkzeuge in der virtuellen Arbeitsumgebung abgelegt. Dabei werden Verknüpfungen der Daten untereinander in den Metadaten gespeichert. Die jeweils finalen Forschungsberichte werden ebenso in der virtuellen Arbeitsumgebung gespeichert. Das Intranet bietet dabei die Funktion an, einen strukturierten Review-Prozess für jedes der zu publizierenden Dokumente zu durchlaufen. Die an einem Bericht oder Publikation beteiligten Wissenschaftler/innen erhalten im Rahmen des Review-Prozesses Zugriff auf das jeweilige Dokument und können Änderungen vorschlagen bzw. mit Hilfe der Kommunikationswerkzeuge über inhaltliche Fragen diskutieren. Abschließend kann das Dokument weiteren Wissenschaftlern/innen zur Verfügung gestellt, publiziert und in der virtuellen Arbeitsumgebung abgelegt werden. Als Format für die Ablage wird der für den Arbeitskontext vereinbarte Standard (z.B. das Open Document Format) verwendet. Bei allen Speicherprozessen werden technische Metadaten der Dokumente verarbeitet und Formatvalidierungen durchgeführt. Der/Die jeweils verantwortliche Wissenschaftler/in ergänzt die Metadaten um Informationen zum Forschungshintergrund und den Autoren. Zusätzlich werden editierbare Versionen der Berichte abgelegt, um diese zu einem späteren Zeitpunkt ggf. für die Publikation einer aktuellen Version anpassen zu können.

### **3. Mögliche Lösungen für Datensicherheit (aus der Expertise)**

Der Anforderung des Datenschutzes an eine physische Lokalität der Daten sowie erforderliche Kapazitäten innerhalb einer Grid-Infrastruktur sowie deren Verarbeitung beim On Demand-Rechnen kann durch Vereinbarung mit einem ausgewählten Anbieter im D-Grid durch ein „Service Level Agreement“ (SLA) Rechnung getragen werden. Hier bietet die Grid Security Infrastructure (GSI, sh. unten) den sicheren Zugang, und die ausgewählten Anbieter die geforderte eingegrenzte Lokalität der Ressourcen<sup>2</sup>.

Um eine eindeutige Identifikation und vertrauliche Kommunikation zu realisieren, setzen Grid-Infrastrukturen auf die so genannte Public Key Infrastructure (PKI)<sup>3</sup>. Die Verwendung von PKI ist ein international anerkannter Standard in wissenschaftlich und kommerziell verteilten IT-Infrastrukturen. Eine PKI basiert darauf, dass jeder Nutzer ein auf seine Person, nach einem vordefinierten Standard, ausgestelltes Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, verwendet. Da diese Schlüssel nicht identisch sind, bezeichnet man dieses Verfahren auch als asymmetrisches Kryptosystem. Es existieren zwei grundlegende Anwendungsszenarien: Verschlüsselung und Signatur.

---

<sup>2</sup> Gerade bei der Erfüllung solcher Anforderungen, die in der Wissenschaft nicht unüblich sind, besteht ein signifikanter Unterschied zwischen einer Grid- und einer Cloud-Infrastruktur.

<sup>3</sup> Chakrabarti, A (2007): Grid Computing Security, Springer, Berlin; Heidelberg; New York.

Die erste Nutzungsmöglichkeit der Verschlüsselung erlaubt anderen Personen dem Schlüsselinhaber Nachrichten zu senden, die mit seinem öffentlichen Schlüssel verschlüsselt worden sind. Der öffentliche Schlüssel kann dazu z.B. auf einer Webseite anderen Nutzern zur Verfügung gestellt werden. Nur der Schlüsselinhaber kann mit seinem privaten Schlüssel die verschlüsselte Nachricht wieder dekodieren und damit den Inhalt einsehen.

Die zweite Nutzungsmöglichkeit der Signatur dient der Authentifizierung und Autorisierung von Nutzern in einer PKI. Zur Authentifizierung sendet ein Nutzer ein so genanntes Zertifikat<sup>4</sup> an die Instanz, die den Nutzer anhand des Zertifikats authentifiziert und damit die angegebene Identität verifiziert.

Ein Zertifikat wird von einer Zertifizierungsstelle i.d.R. gegen persönliche Authentifizierung des Nutzers vor Ort ausgestellt. Ein solches Zertifikat enthält u.a.

- einen Distinguished Name, welcher den Nutzer eindeutig identifiziert<sup>5</sup>,
- die Gültigkeitsdauer<sup>6</sup> des Zertifikats
- den öffentlichen Schlüssel des Nutzers
- eine Signatur des Zertifikatsausstellers (Zertifizierungsstelle, CA)

Wird das Zertifikat zur Authentifizierung von dem Nutzer verwendet, so prüft die authentifizierende Gegenstelle anhand der Signatur und des öffentlichen Schlüssels, ob das Zertifikat gültig ist. Mittels der Gültigkeitsdauer wird die Verwendung eines Zertifikats zeitlich beschränkt.

Da es i.d.R. eine Hierarchie von Zertifizierungsstellen gibt, unterscheidet man zwischen der Certification Authority (CA), die das so genannte Stammzertifikat<sup>7</sup> ausstellt. Und der so genannten Registration Authority (RA), die die Identifikation der Nutzer bei der Ausstellung von Zertifikaten vor Ort gewährleistet. Dabei entsteht eine Vertrauenskette, wobei eine Instanz der jeweils übergeordneten Instanz vertraut. Bei der Verifikation eines Zertifikats kommt zusätzlich die Validation Authority (VA) zum Einsatz. Die VA erhält die Anfragen zur Verifikation und bestätigt die Echtheit eines Zertifikats. Weiterhin wird für die virtuelle Arbeitsumgebung vorgeschlagen, die im Grid existierenden Sicherheitsmechanismen zu nutzen. Dazu gehört der Einsatz der Grid Security Infrastructure in Kombination mit einem VOMRS. Darin nutzt der Anwender eine bestimmte Funktionalität, die zum Beispiel von der virtuellen Arbeitsumgebung über eines der Werkzeuge zur Verfügung gestellt wird. Die Authentifizierung des Nutzers erfolgt über dessen Zertifikat. Die Berechtigungen werden mit Hilfe des Zertifikats, der Grid Security Infrastructure und der VOMRS verifiziert. Dies findet in der virtuellen Ar-

---

<sup>4</sup> Gegenwärtig hat sich für Zertifikate X.509 als Standard etabliert.

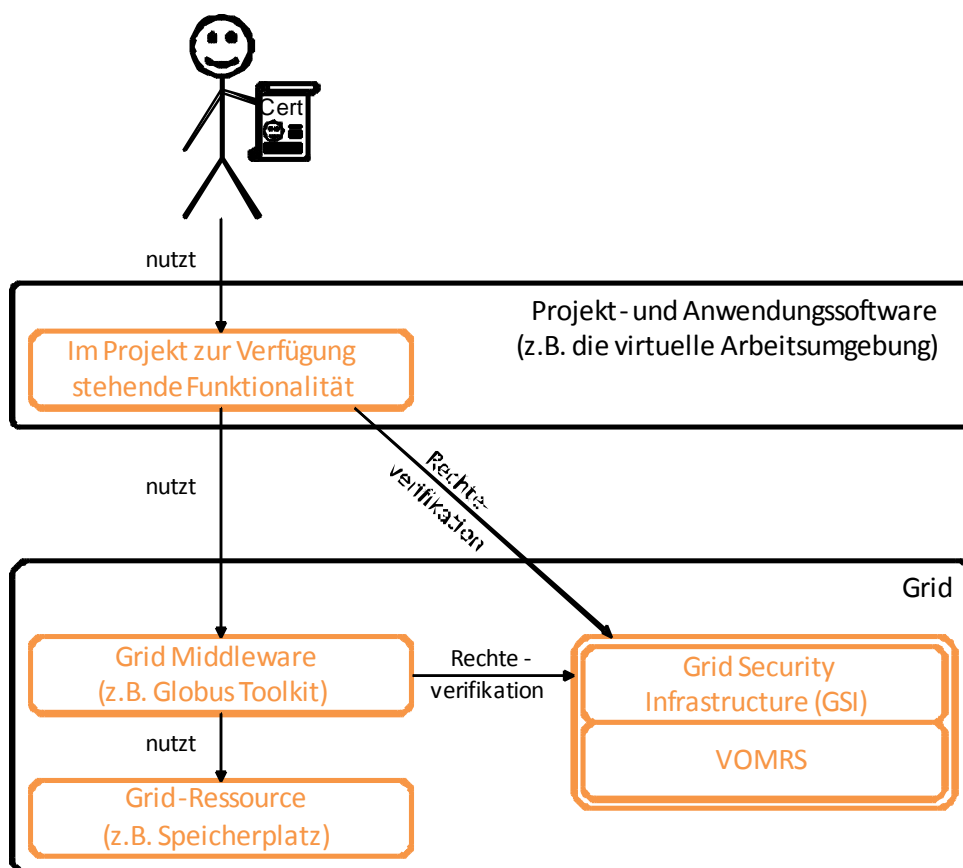
<sup>5</sup> Bei Personen wird i.d.R. der Name, bei Maschinen i.d.R. der Rechnername verwendet.

<sup>6</sup> In D-Grid ist die Gültigkeitsdauer für Nutzer und Maschinen 1 Jahr.

<sup>7</sup> Die CA hält das Stammzertifikat. Alle untergeordneten Instanzen müssen der CA vertrauen. Das Vertrauen in der PKI stützt sich i.d.R. auf das in die Betreiberorganisation gesetzte Vertrauen.

beitsumgebung innerhalb des Systemkerns statt. Liegen die Nutzerrechte vor, so werden die Aktionen ausgeführt. Alle auf Basis der GSI stattfindenden Datentransfers werden verschlüsselt<sup>8</sup> (vgl. Abb.1)

Abbildung 1: Überblick zur Funktionsweise der Grid Security Infrastructure (GSI)



Die Middleware reicht die Überprüfung der Berechtigungen an das lokale System weiter, in dem einem Zertifikat ein lokaler Benutzeraccount zugeordnet ist. Die lokalen Berechtigungen sind für die einzelnen Nutzer (und -gruppen) durch Vereinbarung mit dem Ressourcenprovider festgelegt. So ist auch zu jedem Zeitpunkt eine Nachverfolgbarkeit der Aktionen jedes Grid-Nutzers gegeben. Außerdem können so auch die Aktionen des Benutzers gegenüber den Aktionen anderer Benutzer abgeschottet werden.

Dieses Verfahren entspricht vollständig den im Grid etablierten Standards. Es gibt auch weitere Systeme, die Anwendung finden. Sie sind je nach Anwender-Community verschieden. Die Weiterentwicklung der Sicherheits-Infrastrukturen ist ein elementarer Bestandteil des Grids.

<sup>8</sup> Die zugrunde liegende Technologie baut auf den derzeitigen Standards für gesicherte Netzwerk-Verbindungen auf. Die Referenzimplementationen sind hier OpenSSL (Secure Socket Layer) und Open SSH (Secure Shell).

Der Zugang einzelner Verbundpartner/innen zu den Original- und Arbeitsdaten wird durch eine detailliert definierbare Nutzungsrechteverwaltung kontrolliert. Dazu könnten innerhalb der sozioökonomischen Berichterstattung virtuelle Organisationen (VO) definiert werden. Eine virtuelle Organisation umfasst eine Reihe von Personen, die das Grid nutzen, um ein gemeinsames Ziel zu erreichen. Innerhalb einer solchen Organisation nehmen die Personen unterschiedlichste Aufgaben, Positionen und damit Rollen ein. Außerdem werden die virtuellen Organisationen nicht selten in einzelne Gruppen aufgeteilt. Der Forschungsverbund der sozioökonomischen Berichterstattung wäre zum Beispiel eine solche VO. Die (Unter-)Gruppen der VO können dabei aus den Mitarbeitern/innen der jeweils beteiligten Forschungsinstitutionen, oder aus thematischen Arbeitsgruppen gebildet werden.<sup>9</sup> Die Ausgestaltung des VO Konzepts ist von den Gegebenheiten der Community abhängig.

Zudem kann auf Grundlage der vollständigen Protokollierung von Änderungen an Daten in der virtuellen Arbeitsumgebung sichergestellt und verifiziert werden, dass die maximalen Aufbewahrungszeiten für die Ausgangsdaten (hier SUFs) nicht überschritten werden. Der Forschungsverbund der sozioökonomischen Berichterstattung kann somit gegenüber den FDZ den ordnungsgemäßen Umgang mit den Ausgangsdaten belegen.

Sofern eine Abstimmung mit den entsprechenden FDZ erreicht werden kann, lassen sich SUFs über die virtuelle Arbeitsumgebung bereitstellen. Der Zugang zu bestimmten SUFs via Postweg könnte somit der Vergangenheit angehören. Damit kann eine Entlastung der FDZ und der betroffenen Forscher/innen durch den Einsatz der virtuellen Arbeitsumgebung realisiert werden.

#### **4. Fragen an Forschungsdaneinrichtungen**

##### **Vertragsgestaltung mit Empfänger/in der Daten**

Handelt es sich bei einem Forschungsverbund, der auf einer gemeinsamen IT-Plattform Daten kollaborativ nutzt, aus Ihrer Sicht noch um (lizenzierte) Einzelnutzer/innen? Sieht Ihre Forschungsdaneinrichtung Gruppennutzungsverträge vor? Welche Anforderungen stellen solche Verträge? (Z.B. Rechtsform, Kooperationsvereinbarung?)

Gibt es hierbei Unterschiede zwischen den verschiedenen Nutzungswegen (offsite-Nutzung von SUF, onsite-Nutzung, Datenfernverarbeitung)? Und welche Anforderungen müssten zur Beschreibung des Datenbedarfs für den gesamten Forschungsverbund erfüllt sein?

---

<sup>9</sup> Je nach Anforderungen und Gegebenheiten in der VO können die Mitglieder der VO auch verschiedene Rollen einnehmen, wie z.B. die Rolle eines Datenhalters, die Rolle eines Datenauswerters, und so weiter. Es gibt auch VO-Managementsysteme, die einen Rollen-basierten Zugriff auf Ressourcen ermöglichen.

### **Nutzungsweg Remote Access**

Sind Möglichkeiten des Remote Access in Ihrer Forschungsdateneinrichtung in Planung? Sind Sie an Diskussion darüber beteiligt?

### **Datenschutzkonzepte beteiligter Forschungseinrichtungen**

Welche Anforderungen stellt Ihre Forschungsdateneinrichtung an Zutrittskontrolle, Zugriffskontrolle und Weitergabekontrolle in Datenschutzkonzepten der Forschungseinrichtungen, die Ihre Daten nutzen? Unter welchen Voraussetzungen (z.B. gleichwertige Datenschutzkonzepte der Kooperationspartner/innen) ist eine virtuelle Arbeitsumgebung mit diesen Anforderungen vereinbar?

### **Zugriffskontrolle**

Wären die in der Expertise beschriebenen Lösungen zur Datensicherheit in einer virtuellen Arbeitsumgebung (SLA, Public Key Infrastructure, Grid Security Infrastructure, Virtuelle Organisation mit Nutzungsrechteverwaltung und Nutzungsprotokollierung) ausreichend, um die Anforderungen Ihrer Forschungsdateneinrichtung an Zugriffskontrolle bei kollaborativer Datenauswertung zu erfüllen?

### **Datensicherungsmaßnahmen**

Wie lassen sich Datensicherungsmaßnahmen, die Ihre Forschungsdateneinrichtung in Nutzungsverträgen fordert, auf eine virtuelle Arbeitsumgebung übertragen? Wo sehen Sie hier Konfliktpunkte?

Fiele z.B. die mögliche Vernetzung unter das Verbot des Zugangs von externen Anlagen oder Rechnern? Würde ein festgelegter physikalischer Ort der Daten, der mit einem Service Level Agreement vereinbart werden kann, den Datensicherungsmaßnahmen genügen? Kann eine virtuelle Organisation in einer IT-Plattform als „closed shop“ gelten?

Lässt sich die Vernetzung in einer virtuellen Arbeitsumgebung datenschutzrechtlich von Datenfernverarbeitung abgrenzen?

### **Verbot der Datenzusammenführung**

Erhöht die Zugehörigkeit von Kooperationspartner/innen zu verschiedenen virtuellen Organisationen, die unterschiedliche Datensätze nutzen, die Gefahr unzulässiger Datenzusammenführung?

### **Personelle Nutzungsbeschränkung**

Sind die Personen, die Ihre Daten im Rahmen eines Nutzungsvertrags nutzen, lediglich anzuzeigen oder als Vertragsbestandteil abschließend zu benennen? Wären personelle Veränderungen in einer virtuellen Organisation zur kollaborativen Datennutzung lediglich anzeigepflichtig oder würden sie eine Vertragsänderung bedeuten? Spielt hierbei eine Rolle, ob die Daten Nutzenden Personen in einem Arbeitsverhältnis oder lediglich in einem Kooperationsverhältnis zum Inhaber (zur Inhaberin) des Nutzungsvertrags stehen?

Wie sind die zur Nutzung befugten Personen auf das Datengeheimnis zu verpflichten?

### **Befristung der Nutzung**

Welche Datensätze sind nach Ende einer Nutzungsfrist zu löschen? Welche technischen Anforderungen stellt Ihre Forschungsdateneinrichtung an Löschung? Welche Anforderungen stellen Sie an eine Löschanzeige? Welche Möglichkeiten einer Langzeitarchivierung von Arbeitsdatensätzen für Nachweispflichten, Re-Analysen oder Aktualisierungen bietet Ihre Einrichtung selbst an? Welche Formen der Langzeitarchivierung sind mit den Löschverpflichtungen vereinbar?

### **Zweckbindung der Datennutzung**

Welche Anforderungen stellt Ihre Forschungsdateneinrichtung an den Nachweis unabhängiger wissenschaftlicher Forschung, an die Darstellung des Forschungsvorhabens und an die Begründung des Datenbedarfs? Sind bei Änderungen des Forschungsdesigns, des methodischen Ansatzes oder der Forschungsanteile von Kooperationspartner/inne/n Vertragsänderungen erforderlich? Verändert die Datennutzung in einem virtuell vernetzten Forschungsverbund die Anforderungen an hinreichend bestimmte Angaben zur Zweckbindung der Datennutzung?

### **Anforderungen an Auswertungsprogramme**

Welche Anforderungen stellen Sie bei der Datenfernverarbeitung und bei Gastaufenthalten an den Aufbau von Auswertungsprogrammen?

Welche Anforderungen stellen Sie an den Aufbau von Auswertungssyntax und an die Dokumentation von Auswertungsprogrammen? Gelten diese auch für off-site-Nutzung von SUFs?

### **Metadaten**

Stellt Ihre Forschungsdateneinrichtung Anforderungen an Metadaten über die Forschungsergebnisse der Datennutzer/innen?

Unterliegen datensatzbeschreibende Informationen auch Beschränkungen hinsichtlich der Weitergabe?