

1

Working Paper
2024

KonsortSWD



Konsortium für die
Sozial-, Verhaltens-, Bildungs- und
Wirtschaftswissenschaften

Vertragliche Grundlagen zur Teilnahme am RDCnet

Version 2.0

Neil Murray und Jan Goebel



Oktober 2024

www.konsortswd.de

Vertragliche Grundlagen zur Teilnahme am RDCnet

Version 2.0

Neil Murray und Jan Goebel
DIW Berlin (SOEP)

Berlin, Oktober 2024

Abstract

Forschende der Sozial-, Bildungs-, Verhaltens- und Wirtschaftswissenschaften arbeiten mit verschiedenen Datentypen, die häufig aufgrund rechtlicher oder ethischer Beschränkungen besonders sensibel sind und oftmals nicht originär für wissenschaftliche Zwecke erhoben wurden. Die Projekte des KonsortSWD¹ haben zum Ziel, Forschenden und Institutionen, die zunehmend in multi- und interdisziplinären Projekten zusammenarbeiten, Unterstützung bei ihrem Forschungsdaten-management (FDM) anzubieten.

Ein Teilprojekt des KonsortSWD bildet das RDCnet (TA.2-M.2) welches dazu dient, Gastwissenschaftsarbeitsplätze (GWAP) teilnehmender Forschungsdatenzentren in einem Netzwerk von gesicherten Datenzugangsstellen zu vernetzen. Anstatt dass Forschende zwingend zu einem bestimmten FDZ reisen müssen, um deren Daten zu analysieren, können sie durch das RDCnet aus einer Auswahl an teilnehmenden Instituten den für sie passendsten Standort wählen. Durch den erleichterten Zugang kann die Anzahl der Datennutzenden erhöht werden, wobei die Kontrolle über die letztendliche Distribution der Datensätze weiterhin den Datenanbietern obliegt, um somit auch individuelle Standards der Datensicherheit gewährleisten zu können.

Im vorliegenden Arbeitspapier wurden in Zusammenarbeit mit zehn im Rahmen des KonsortSWD akkreditierten FDZ vertragliche Grundlagen für die Teilnahme am RDCnet definiert, die notwendig sind, um ein entsprechendes Vertrauensverhältnis, organisatorische Leitlinien und eine rechtliche Absicherung zwischen den teilnehmenden Institutionen zu schaffen. Das Papier umfasst eine multilaterale Kooperationsvereinbarung sowie technische und organisatorische Maßnahmen der GWAP.

<https://doi.org/10.5281/zenodo.13827792>

¹ Siehe Konsortialantrag in Adena et al. 2020.

Inhaltsverzeichnis

Abkürzungsverzeichnis & Definitionen	3
Einleitung RDCnet	5
Prozessbeschreibung des RDCnet	7
Übersicht: Zuständigkeiten und Leistungen der Parteien.....	9
Daten-Partei.....	9
GWAP-Partei.....	10
Kooperationsvereinbarung	12
Präambel	12
§ 1 Ziel und Gegenstand der Zusammenarbeit.....	13
§ 2 Definitionen	13
§ 3 Voraussetzungen und Ablauf der Datennutzung im RDCNet.....	14
§ 4 Kooperationsbeiträge der Kooperationspartner	15
§ 5 Kosten	16
§ 6 Haftung.....	17
§ 7 Laufzeit der Vereinbarung und Kündigung	17
§ 8 Weitere Bestimmungen.....	18
Anlage 1: Technische und organisatorische Maßnahmen zum Schutz der gastwissenschaftlichen Arbeitsplätze	19
(1) Raumsicherung	19
(2) Technische Kriterien:	20
Anlage 2: Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes	22
Literaturverzeichnis	23

Abkürzungsverzeichnis & Definitionen

1. Abkürzungen

FDZ	Forschungsdatenzentrum
GWAP	Gastwissenschaftsarbetsplatz
RDCnet	Research Data Center Network
TOM	Technisch organisatorische Maßnahmen
VDI	Virtual Desktop Infrastructure
OTP	One-Time Password

2. Definitionen

Daten-Partei	Die Institution, deren Forschungsdaten an den Arbeitsplätzen der jeweils anderen GWAP-Partei zugänglich gemacht werden.
GWAP-Partei:	Die Institution, an der den Forschenden der Zugang zu Forschungsdaten anderer Daten-Parteien mittels Fernzugang von einem gesicherten GWAP aus ermöglicht wird.
Datensicherheitsraum	Gesicherte Räumlichkeit, in welcher sich die Arbeitsplatz der GWAP-Partei befinden.
Forschende	Personen, die den Service des RDCnet nutzen und per Remote Access die Forschungsdaten einer Daten-Partei vom Arbeitsplatz einer GWAP-Partei analysieren.
Forschungsdaten	Bezeichnet die Daten, die von den Daten-Parteien bereitgestellt und von den Forschenden analysiert werden. Im Kontext des RDCnet handelt es sich dabei um sensible Forschungsdaten, die den Forschenden nicht per Download angeboten werden können, da sie in der Regel ein hohes Maß an potenzieller

	Rückidentifizierbarkeit zulassen und deshalb die Server der Daten-Parteien nicht verlassen dürfen.
Gastwissenschafts-arbeitsplatz	Bezeichnet den Arbeitsplatz, von welchem Forschende per Remote Access die Forschungsdaten der Daten-Parteien bearbeiten können. Ein Gastwissenschaftsarbeitsplatz befindet sich stet innerhalb eines Datensicherheitsraums und ist mit einem restriktiv konfigurierten Terminal/Thin Client ausgestattet.
Kooperationspartner	Jede Institution die im RDCnet als GWAP- oder Daten-Partei teilnimmt.
OTP	Werden neben dem regulären Benutzerpasswort als zusätzliche Authentifizierungsstufe verwendet.
Remote Access	Allgemeiner Fernzugriff von einem lokalen Computer auf einen entfernten Rechner/Server. Die Daten auf die dabei zugegriffen wird, verlassen zu keinem Zeitpunkt physisch die Rechner/Server des Anbieters.
Remote Desktop	Spezifischer als der Remote Access, bezeichnet der Remote Desktop einen bereitgestellten Desktop, der per Fernzugriff gesteuert werden kann. Dabei werden jedoch nur das Bild und die Eingabe von Tastatur und Maus übertragen.
Thin Client:	Ein Computer, der über ein Netzwerk mit einem Server verbunden wird und dessen Ressourcen nutzt. Die Hardware eines Thin Client erlaubt nur die Darstellungs- und Eingabefunktionen.
VDI	Eine Remote Desktop Lösung die von VMware angeboten wird.

Für eine detaillierte Beschreibung der Begrifflichkeiten und Arten des Remote Access siehe Schiller et al. (2017)

Einleitung RDCnet

Für die empirische Forschung im Bereich der Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften sind Forschende darauf angewiesen, auf entsprechende Daten (z. B. Haushalts- oder Personenumfragen) zugreifen zu können. In den meisten Fällen werden solche Daten durch akkreditierte Forschungsdatenzentren (FDZ) verschiedener wissenschaftlicher Forschungsinstitute generiert. Die Art des Zugangs hängt jedoch vom Grad der Anonymisierung ab, um die Identität von Befragten zu schützen. So können vollständig anonymisierte Datensätze von den Forschenden in der Regel auch direkt von zu Hause genutzt werden, wenn entsprechende Datennutzungsverträge unterschrieben wurden.

Sofern Daten jedoch nur eine schwache oder gar keine Anonymisierung vorweisen, sind sie nur an Gastwissenschaftsarbeitsplätze (GWAP) der jeweiligen Institute vor Ort zugänglich, um gesetzliche Vorgaben, wie die des Bundesdatenschutzgesetzes, oder vertragliche Regelung mit externen Datengebern bzgl. des Vertrauensschutzes einzuhalten. Ein GWAP definiert sich also als dedizierter Arbeitsplatz für Forschende, an dem sensible Daten eines FDZ zugänglich gemacht werden können.

Ein solcher GWAP befindet sich in einer gegen unbefugten Zugriff geschützten Räumlichkeit (Datensicherheitsraum) und verfügt über eine Hard- und Softwareausstattung, die es verhindert, Daten ohne Prüfung durch das Institut nach außen zu tragen. In der Regel werden hierfür Thin-Clients oder Computer genutzt, mit denen das Kopieren, Speichern oder Versenden von Daten nicht möglich ist und die keinen Zugang zum Internet besitzen. Zudem wird der Zutritt der Forschenden i. d. R. durch geschultes FDZ-Personal kontrolliert. Die eigentliche Bearbeitung bzw. Analyse der Daten erfolgt auf einem speziell gesicherten Datenserver, der nur von diesem Thin-Client oder Computer aus zugänglich ist.

Diese Lösung garantiert zwar Datensicherheit und Vertrauensschutz, führt jedoch bei den Forschenden zu einem beträchtlichen Kosten und Zeitaufwand, da die Daten nur bei dem Daten Institut vor Ort zugänglich sind und somit unter Umständen eine Reise quer durch Deutschland notwendig ist.

Innerhalb des RDCnet sollen die GWAP verschiedener akkreditierter FDZ in einem nationalen² Netzwerk verknüpft werden. So können sensible Daten durch Forschende nicht nur am heimischen FDZ, sondern an allen teilnehmenden FDZ vor Ort bearbeitet werden. Hierfür stellt jedes teilnehmende FDZ innerhalb des RDCnet einen eigenen GWAP zur Verfügung und erhält dadurch die Möglichkeit eigene Daten auch an den GWAP anderer FDZ zugänglich zu machen.

Ziel ist es, ein Verfahren und eine Netzwerkstruktur zu implementieren, mit dem es möglich ist, die Daten eines FDZ A von dem GWAP eines FDZ B zu bearbeiten, ohne dass die Daten den heimischen Server des FDZ A physisch verlassen. So wird gewährleistet, dass die Daten FDZ

2 Für Informationen hinsichtlich der Implementierung sowie der Bereitstellung vertraglicher Grundlagen von **internationalen** Fernzugriffen auf vertraulichem Daten verweisen wir auf ein Projekt der Social Sciences & Humanities Open Cloud (SSHOC). Siehe Woollard et al. (2021).

weiterhin selbst für die Sicherheit ihrer Datenserver verantwortlich sind und stets die Entscheidungsmacht darüber haben, von wo die Daten bearbeitet werden können. Jedem FDZ obliegt auch weiterhin die Entscheidung, wer die Daten nutzen darf- also nach welchen Kriterien und mit welchen Personengruppen Datennutzungsverträge³ geschlossen werden.

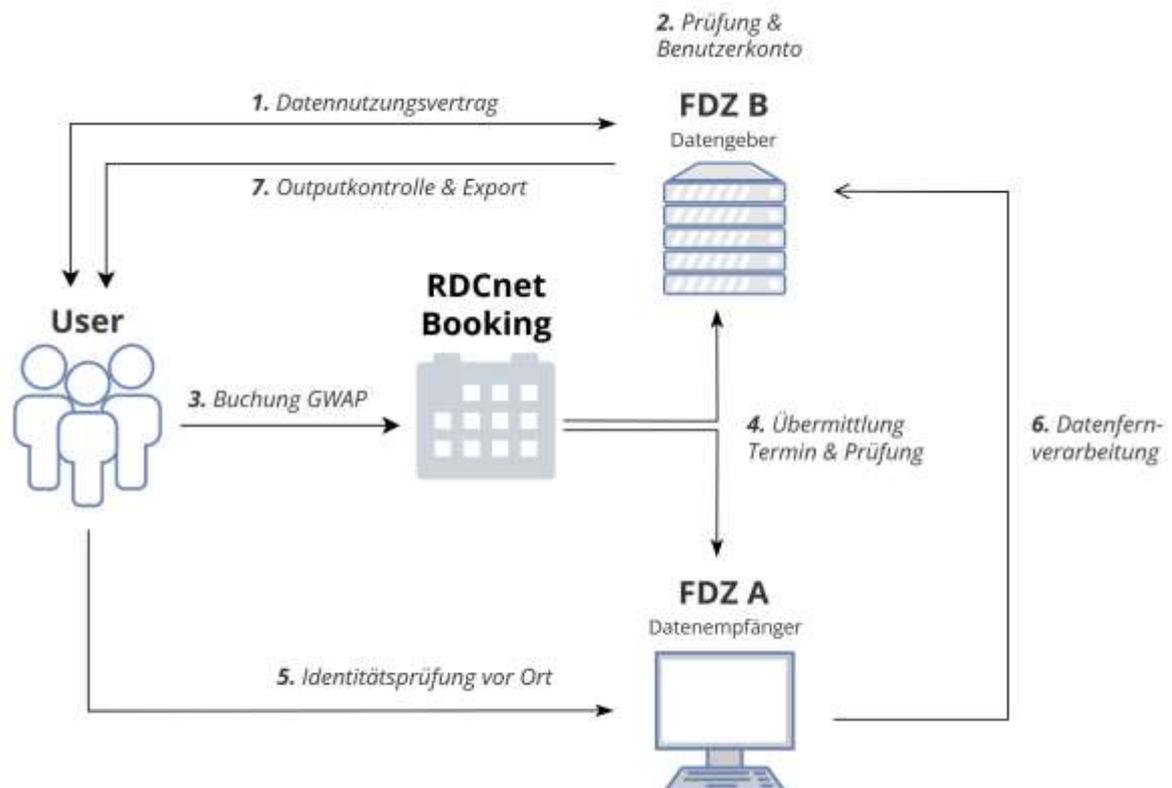
Neben den technischen Rahmenbedingungen ist eine vertragliche Grundlage zwischen den teilnehmenden FDZ notwendig, um ein entsprechendes Vertrauensverhältnis, organisatorische Leitlinien und eine rechtliche Absicherung zu schaffen. Dies wird durch die Definition von Teilnahmeregelungen und der Festlegung von Mindestsicherheitskriterien der GWAP umgesetzt. Das vorliegende Dokument umfasst hierfür eine multilaterale Kooperationsvereinbarung sowie technische und organisatorische Maßnahmen in Bezug auf die Ausgestaltung der GWAP. Neben der juristischen Erarbeitung des Kooperationsvertrags, basiert das Dokument auf einer Evaluation bereits bestehenden TOM verschiedener nationaler Datenzentren, die in Zusammenarbeit⁴ mit zehn beteiligten FDZ erweitert und präzisiert wurden. Zudem wurde als strukturelle und inhaltliche Vorlage auf die Handreichung „Framework and contract for international data use agreements on remote access to confidential data“ (Woollard et al., 2021) der SSHOC zurückgegriffen.

3 Im Rahmen des KonsortSWD wurde ein Mustervertrag zur Datennutzung erarbeitet, der bei Bedarf genutzt werden kann. Siehe Schallaböck et al. 2022.

4 Vielen Dank an: Christian Aßmann (LifBi), Daniel Fuß (LifBi), Sebastian Wichert (ifo), Philipp Breidenbach (RWI), Jara Kampmann (gesis), Deborah Wiltshire (gesis), Sandra Gottschalk (ZEW), Nikos Askitas (IZA), Daniel Buck (DZHW), René Wilke (aviDa), Kati Mozygemba (SOCIUM/FDZ Qualiservice), Thomas Hollacher (DIW)

Prozessbeschreibung des RDCnet

Im folgenden Beispielprozess werden die benötigten Arbeitsschritte der teilnehmenden Parteien zur Nutzung des RDCnet erläutert. In diesem Szenario wird davon ausgegangen, dass Forschende die Daten des FDZ B (Daten-Partei) am GWAP des FDZ A (GWAP-Partei) bearbeiten wollen.



Prozessschritte:

1. Die Forschenden stellen bei FDZ B einen Antrag zu Datennutzung. Die Gestaltung und Form des Antrags obliegt alleinig dem FDZ B.
2. FDZ B prüft den Antrag nach den eigenen Kriterien und bestätigt den Forschenden die Berechtigung zur Datennutzung oder lehnt diese ab.
3. Verfügen Forschende über einen gültigen Datennutzungsvertrag mit FDZ B, können sie auf der Buchungsplattform des RDCnet eine Buchungsanfrage für einen GWAP bei teilnehmenden Partner Institutionen stellen – in diesem Beispiel bei FDZ A. Termine sind frühestens einen Monat vor Antritt buchbar.

4. Nachdem die Forschenden eine Buchungsanfrage gestellt haben, werden sowohl die Daten- als auch die GWAP-Partei über die Anfrage durch automatisierte E-Mails informiert. Dabei werden den involvierten Parteien Informationen zu den Forschenden (Name, Kontakt, Forschungsthema, Kennung Datennutzungsvertrag) als auch Informationen zur Buchung (Datum, Anzahl gebuchter Tage) übermittelt. Die Daten-Partei- in diesem Fall FDZ B- muss nun die Buchung innerhalb der Buchungsplattform bestätigen. Hierfür erhält jeder Kooperationspartner ein entsprechendes Benutzerkonto für die Buchungsplattform, mit dem auf die angefragten Buchungen zugegriffen werden kann. FDZ B prüft nun, ob für die Forschende oder den Forschenden ein gültiger Datennutzungsvertrag vorliegt und bestätigt die Buchung entsprechend oder storniert die Buchung, falls kein gültiger Vertrag vorliegt. Die GWAP-Partei – in diesem Fall FDZ A- muss den Termin lediglich in ihr System/Kalender eintragen, sodass bei Antritt der Forschenden, der GWAP verfügbar ist und die Identität durch Personal der GWAP-Partei geprüft werden kann. Wird der Termin durch die Forschenden oder durch die Daten-Partei storniert, erhalten alle beteiligten Parteien per E-Mail eine Stornierungsinformation.
5. Wird die Buchungsanfrage durch FDZ B angenommen, muss den Forschenden ein Benutzerkonto auf einem Server des FDZ B erstellt werden. Das Benutzerkonto muss durch einen Benutzernamen und Passwort gesichert sein. Die Zugangsdaten des Benutzerkontos sind spätestens bis zum gebuchten Termin vom FDZ B an die Forschenden zu übermitteln. Außerdem hat FDZ B selbst dafür zu sorgen, dass das Benutzerkonto nach Ablauf der im Datennutzungsantrag festgelegten Vertragsdauer, unzugänglich wird. Wie die virtuelle Umgebung des Benutzerkontos gestaltet ist (z.B. welche Software verfügbar ist, wie die Ordnerstruktur gegeben ist usw.) entscheidet FDZ B selbst.

Ergänzung 2-Faktor-Authentifizierung: Jede Daten-Partei kann selbst entscheiden, ob sie den Forschenden einen zusätzlichen Authentifizierungsprozess einrichtet, wie beispielsweise ein OTP. Für diesen Faktor werden im RDCnet jedoch keine Vorgaben gemacht, da ausschließlich die Daten-Partei dafür verantwortlich ist und hierzu keine Informationen mit der GWAP-Partei ausgetauscht werden müssen. Wenn eine Daten-Partei die Notwendigkeit sieht, einen weiteren Faktor einzurichten, der durch das Personal der GWAP-Partei getätigt werden muss, wie beispielsweise ein zusätzliches Passwort, ist darauf zu achten, dass der GWAP-Partei dadurch kein zusätzlicher Aufwand entsteht, außer der Eingabe des Passworts am Endgerät. Eine Möglichkeit wäre beispielsweise die Nutzung von Token-Generatoren, die durch die Daten-Partei eingerichtet und jeder GWAP-Partei ausgegeben werden.

6. Bevor Forschende den Datensicherheitsraum zum gebuchten Termin betreten dürfen, muss FDZ A eine Identitätskontrolle (amtliches Ausweisdokument) durchführen und gewährleisten, dass alle technischen und organisatorischen Maßnahmen (TOM) zur Sicherung des GWAP umgesetzt sind und während der Nutzungsdauer eingehalten werden. Zudem müssen die Forschenden auf die im Datensicherheitsraum und am GWAP geltenden Sicherheitsregelungen hingewiesen werden. Diese Einweisung und die

Identitätskontrolle sind durch die Unterschriften eines/r FDZ-Mitarbeiters/in der GWAP-Partei und der Forschenden auf dem Formular „Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes“ (siehe Anhang 2) zu protokollieren und zu bestätigen. Anschließend kann eine Zugangskarte/Schlüssel ausgehändigt werden oder der Raum wird manuell durch Mitarbeiter*innen der GWAP-Partei geöffnet. Zudem sollte kommuniziert werden, an wen sich Forschende wenden können, falls Fragen hinsichtlich der Nutzung des Terminals oder des Datensicherheitsraumes gibt.

7. Forschende können sich nun am GWAP mithilfe der übermittelten Zugangsdaten einloggen und auf die für sie eingerichtete virtuelle Umgebung am Server des FDZ B zugreifen.
8. Beenden Forschende die Datenbearbeitung, setzen sie FDZ B darüber in Kenntnis. Mitarbeitende Personen des FDZ B können nun die Output Kontrolle vornehmen. Nach welchen Kriterien diese ausgeführt wird obliegt FDZ B. Danach übermittelt FDZ B die Ergebnisse Kontrolle zurück an die Forschenden. Dabei kann FDZ B selbst bestimmen auf welche Weise die Übermittlung vorgenommen wird.

Übersicht: Zuständigkeiten und Leistungen der Parteien

Daten-Partei

1. **Remote Access:** Die Daten-Partei implementiert eine Serverinfrastruktur, die eine sichere Remote Desktop Verbindung von den Arbeitsplätzen der GWAP-Parteien aus ermöglicht.
2. **Datennutzungsvertrag:** Die Daten-Partei stellt Forschenden Anträge zur Datennutzung bereit und prüft diese Anträge nach eigenen Kriterien.
3. **Buchungsanfragen:** Die Daten-Partei prüft Buchungsanfragen der Forschenden, die über die Buchungsplattform des RDCnet eingehen, und bestätigt diese, falls ein gültiger Datennutzungsvertrag vorliegt, oder lehnt sie ab.
4. **Benutzerkonto:** Die Daten-Partei erstellt für die Forschenden, deren Datennutzungsantrag und Buchungsanfrage angenommen wurden, ein entsprechendes Benutzerkonto für den sicheren Remote Access mit einem Benutzernamen und Passwort (optional OTP) und übermittelt den Forschenden diese Daten durch eine sichere Methode spätestens bis zum Termin der GWAP-Nutzung.
5. **Authentifizierung:** Falls eine zusätzliche Authentifizierung durch das Personal der GWAP-Partei erforderlich ist (z.B. in Form eines OTP), ist diesem das entsprechende Passwort spätestens bis zur GWAP-Nutzung der Forschenden zu übersenden.
6. **Support:** Die Daten-Partei übermittelt den Forschenden Kontaktinformationen (Telefonnummer, E-Mail) für Supportanfragen bezüglich der Forschungsdaten, des

erstellten Benutzerkontos oder anderer Fragen, die in den Aufgabenbereich der Daten-Partei fallen.

7. **Output Kontrolle:** Die Daten-Partei ist selbst für die Kontrolle der Ergebnisse und deren Übermittlung an die Forschenden verantwortlich.
8. **Sperrung Benutzerkonto:** Nach Ablauf des Datennutzungsvertrags hat die Daten-Partei dafür zu sorgen, dass das entsprechende Benutzerkonto unzugänglich gemacht wird.

GWAP-Partei

1. **Installation GWAP:** Die GWAP-Partei installiert einen für das RDCnet dedizierten Arbeitsplatz in Form eines Thin Clients innerhalb eines Datensicherheitsraums.
2. **Remote Access:** Die GWAP-Partei richtet sichere Remote Access Verbindungen von den Thin Clients zu den Servern der Daten-Parteien ein.
3. **Sicherheit:** Die GWAP-Partei implementiert die in Anhang 1 (Technische und organisatorische Maßnahmen zum Schutz der gastwissenschaftlichen Arbeitsplätze) definierten Kriterien zur Sicherung des Arbeitsplatzes und des Datensicherheitsraumes.
4. **Buchungsanfragen & Zugang:** Die GWAP-Partei erfasst Buchungsanfragen der Forschenden, die über die Buchungsplattform des RDCnet eingehen, in ihrem System und stellt sicher, dass der GWAP zum gebuchten Termin für die entsprechenden Forschenden verfügbar ist. Die GWAP-Partei ist nicht berechtigt, den Forschenden den Zugang zu den RDCnet-GWAP zu verweigern, es sei denn, es liegt eine technische Störung oder Personalausfall vor, die es unmöglich machen, die Kontrollpflicht einzuhalten.
5. **Zugangskontrolle:** Die GWAP-Partei überprüft die Identität der Forschenden anhand eines Lichtbildausweises, bevor diese den Datensicherheitsraum betreten dürfen, und gewährt nur autorisierten Personen Zugang. Zudem informiert sie die Forschenden über die geltenden Regelungen innerhalb des Datensicherheitsraums. Die Identitätskontrolle und Einweisung müssen durch die Unterschrift der Forschenden und einer Mitarbeiterin oder eines Mitarbeiters der GWAP-Partei auf dem Formular "Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes" (siehe Anhang 2) protokolliert werden, bevor Forschenden der Zugang gewährt wird.
6. **Authentifizierung:** Falls eine zusätzliche Authentifizierung durch das Personal der GWAP-Partei erfolgen muss (zum Beispiel in Form eines OTP), darf das von der Daten-Partei übermittelte Passwort nicht mit anderen Personen geteilt werden, auch nicht mit dem Forschenden selbst.
7. **Kontrollen:** Das Personal der GWAP-Partei führt physische Kontrollen zur Einhaltung der im Datensicherheitsraum geltenden Regelungen durch. Sollten Verstöße gegen diese Regelungen festgestellt werden, ist die Daten-Partei darüber zu informieren.

8. **Support:** Die GWAP-Partei benennt eine Ansprechperson, an die sich die Forschenden bei Fragen zum Datensicherheitsraum oder zum GWAP bzw. zum Thin Client wenden können.
9. **Wartung Technik:** Die GWAP-Partei ist selbst für die Wartung der Thin Clients und der im Datensicherheitsraum benötigten Technik verantwortlich. Sollten Probleme bei der Remote-Access-Verbindung zu einer Daten-Partei auftreten, ist diese darüber zu informieren.

Kooperationsvereinbarung

Institution A

vertreten durch _____,

Adresse

Nachstehend **Institution A**

und

Institution B

vertreten durch _____,

Adresse

Nachstehend **Institution B**

und

Institution C

vertreten durch _____,

Adresse

Nachstehend **Institution C**

schließen folgende Kooperationsvereinbarung.

Präambel

Die Kooperationspartner wollen im Rahmen des KonsortSWD Projekts

RDCnet: Implementierung eines Netzwerkes sicherer Gastwissenschaftsarbeitsplätze

die jeweils von ihnen betriebenen Forschungsdatenzentren (FDZ) zu einem nationalen Netzwerk an FDZ verknüpfen, um Forschenden über Gastwissenschaftsarbeitsplätze (GWAP) einen vereinfachten Zugang zu den Forschungsdaten der teilnehmenden Kooperationspartner zu verschaffen. Im Rahmen des RDCnet sollen Forschende über eine sichere Fernverbindung (Remote Desktop) von einem GWAP eines Kooperationspartners aus Zugang zu Forschungsdaten – auch datenschutzrechtlich sensible Daten – anderer Kooperationspartner erhalten, ohne dass die Forschungsdaten physisch den Server, auf dem sie vertrieben werden, verlassen.

Im Rahmen des Projekts haben die Kooperationspartner die organisatorischen und technischen Maßnahmen festgelegt, die dabei zum Schutz der – ggfls. Auch personenbezogenen –

Forschungsdaten zu beachten und von den einzelnen Kooperationspartnern zu gewährleisten sind. Außerdem wollen sie die Kriterien zur Sicherung der GWAP ihrer Institution miteinander kompatibel machen.

Die Kooperationspartner erfüllen mit der Kooperation ausschließlich Zwecke entsprechend ihren Grundlegendokumenten und nehmen ihre Kooperationsaufgaben zur Erreichung des gemeinsamen Kooperationsziels in jeweils eigener wissenschaftlicher Verantwortung und Unabhängigkeit wahr. Die Rechtsbeziehungen ihrer Zusammenarbeit in diesem wissenschaftlichen Projekt regeln sie wie folgt:

§ 1 Ziel und Gegenstand der Zusammenarbeit

(1) Ziel der Kooperation ist die Schaffung eines vereinfachten Datenzugangs zum Forschungsdatenangebot, welches an den Standorten der kooperierenden Institutionen verfügbar ist. Der Zugang erfolgt von den GWAP aus, die mit gesonderten Rechnern (z.B. Thin Clients) ausgerüstet werden, mittels eines gesicherten Fernzugangs (Remote Desktop).

(2) Jeder Kooperationspartner führt auf einer öffentlich einsehbaren Liste - unter anderem auf seiner Homepage - die GWAP-Parteien auf, an deren Arbeitsplätzen die eigenen Forschungsdaten zugänglich gemacht werden können.

(3) Im Rahmen dieses Projekts werden die Forschungsdaten der Kooperationspartner ausschließlich zu wissenschaftlichen Forschungszwecken zugänglich gemacht.

(4) Klagbare Ansprüche der Forschenden oder einer Institution auf einen Zugang zu den Forschungsdaten der Kooperationspartner bestehen gegenüber den Kooperationspartnern aus dieser Kooperationsvereinbarung nicht.

§ 2 Definitionen

(1) Im Sinne dieses Vertrages ist

- **„GWAP-Partei“** die Institution, an dem Forschenden der Zugang zu Forschungsdaten anderer Kooperationspartner mittels Fernzugang von einem gesicherten GWAP aus ermöglicht wird.
- **„Daten-Partei“** die Institution, deren Forschungsdaten an den GWAP der jeweils anderen Kooperationspartner zugänglich gemacht werden.
- **„Kooperationspartner“** jede Institution die im RDCnet als GWAP- oder Daten-Partei teilnimmt.
- **Forschende:** Personen, die den Service des RDCnet nutzen und per Remote Access die Forschungsdaten einer Daten-Partei vom Arbeitsplatz einer GWAP-Partei analysieren.

(2) Jeder Kooperationspartner übernimmt im Rahmen dieses Projekts die Aufgaben und Funktionen der GWAP-Partei. Darüber hinaus kann jeder Kooperationspartner als Daten-Partei tätig werden, hierzu besteht jedoch keine vertragliche Verpflichtung.

§ 3 Voraussetzungen und Ablauf der Datennutzung im RDCNet

(1) Alle Kooperationspartner verpflichten sich zur Nutzung und Teilnahme an der Buchungsplattform des RDCnet. Der Austausch von Nutzerdaten und die Terminbuchung für die GWAP finden ausschließlich über die Buchungsplattform des RDCnet statt.

(2) Für die Nutzung des RDCnet reichen Forschende zunächst einen Antrag zur Datennutzung bei der entsprechenden Daten-Partei ein, welcher von dieser geprüft und beschieden wird. Die Kriterien und Auflagen, nach denen ein Datennutzungsvertrag angenommen wird, obliegen jeder Daten-Partei selbst.

(3) Nachdem der Antrag zur Datennutzung durch die Daten-Partei akzeptiert wurde, können Forschende über die Buchungsplattform des RDCnet eine Buchungsanfrage für die Nutzung eines Arbeitsplatzes an einer der verfügbaren GWAP-Parteien stellen. Die getätigte Buchungsanfrage wird über die Buchungsplattform sowohl an die Daten- als auch an die GWAP-Partei übermittelt⁵. Die Daten-Partei erhält die Buchungsanfrage per E-Mail, und bestätigt die Buchungsanfrage, wenn der Forschende über ein gültigen Datennutzungsvertrag verfügt. Die GWAP-Partei hat dafür Sorge zu tragen, dass der gebuchte GWAP zum übermittelten Termin verfügbar ist.

(4) Genehmigt die Daten-Partei die Buchungsanfrage, so hat sie dafür Sorge zu tragen, dem Forschenden spätestens bis zum übermittelten Termin der GWAP-Nutzung ein Benutzerkonto für den Remote Zugang zu erstellen und dem Nutzenden alle relevanten Parameter zu übermitteln (Benutzername, Passwort ...)

(5) Die Forschenden nutzen die Forschungsdaten der Daten-Partei vom Arbeitsplatz der GWAP-Partei aus unter Beachtung der Datensicherheitsstandards der GWAP-Partei gemäß Anlage 1. Die GWAP-Partei führt eine Kontrolle der Identität des Forschenden durch und achtet auf die Einhaltung der Datensicherheitsstandards. Die Identitätsprüfung wird durch die Unterzeichnung des Dokuments "Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes" (siehe Anhang 2) protokolliert.

(6) Nach Abschluss der Datenbearbeitung durch die Forschenden nimmt die Daten-Partei die Output-Kontrolle nach Maßgabe seiner Kriterien und Regelungen vor und übermittelt bei erfolgreicher Kontrolle die Ergebnisse an die Forschenden.

(7) Im Übrigen gelten die technischen Spezifizierungen gemäß der Anlage 1. Bei Zweifelsfällen und Unstimmigkeiten ist diese ausschlaggebend.

⁵ Übermittelt werden dabei: Namen des Forschenden, Kontaktinformationen, Titel des Forschungsprojekt, Kennung des Datennutzungsvertrag und der Termin für den der GWAP gebucht wurde.

§ 4 Kooperationsbeiträge der Kooperationspartner

(1) Jeder Kooperationspartner erbringt die Kooperationsbeiträge, die sich aus dem in § 3 dargestellten Ablauf einer Datennutzung ergeben.

(2) Jede GWAP-Partei stellt sicher, dass den Forschenden, ein Ansprechpartner für die Anweisung zur Nutzung der GWAP, sowie zur Beantwortung potenzielle Fragen hinsichtlich der Terminals oder des Datensicherheitsraum zur Verfügung steht.

(3) Jede Daten-Partei stellt sicher, dass den Forschenden der Kontakt zu einem Ansprechpartner übermittelt wurde, an den sich die Forschenden bei Fragen hinsichtlich der Forschungsdaten, des bereitgestellten virtual Desktops oder der Benutzerdaten wenden kann.

(4) Jeder Kooperationspartner richtet an seiner Institution zumindest einen geschützten Raum mit einem GWAP einschließlich eines dafür eingerichteten Rechners (Thin Clients) ein, über den der Zugang zu den Forschungsdaten der Kooperationspartner mittels einer gesicherten Fernverbindung zur Verfügung gestellt wird. Jeder Kooperationspartner ist für die Einrichtung der GWAP sowie die Anschaffung und Installation der Thin Clients und der erforderlichen Software verantwortlich. Jedem Kooperationspartner obliegen zudem die Wartung der Software und die Reparaturen der Hardware. Zudem dürfen den Forschenden keine Kosten für die Nutzung des GWAP auferlegt werden. Unberührt bleibt das Recht der Daten-Partei, von Forschenden ein Entgelt für die Bereitstellung der Daten zu verlangen.

(5) Jeder Kooperationspartner definiert als Daten-Partei nach seinen Standards Verbindungen, die auf den jeweiligen datenspeichernden Servern erlaubt werden und behält damit die Verfügungshoheit in Bezug auf die von ihm zur Verfügung gestellten Daten.

(6) Der Remote Access erfolgt standardisiert über die Nutzung von VMware Horizon. Die konkrete Umsetzung der hierfür erforderlichen Serverinfrastruktur innerhalb der Institution einer Daten-Partei liegt in der Verantwortung jeder einzelnen Daten-Partei. Die GWAP-Partei stellt sicher, dass der Remote Access von den Thin Clients standardisiert über die Nutzung des „VMware Horizon Client“ erfolgen kann. Die Nutzung einer davon abweichenden Remote Access Software durch eine Daten-Partei, bedarf der Zustimmung aller Kooperationspartner. Die Implementierung einer solchen abweichenden Software sollte für die GWAP-Partei keinen signifikant größeren Aufwand als die Implementierung von VMware Horizon bedeuten.

(7) Jede Daten-Partei stellt Forschenden Antragsformulare zur Nutzung seiner Forschungsdaten zur Verfügung.

(8) Die Daten-Parteien prüfen und bescheiden die Datennutzungsanträge von Forschenden nach ihren eigenen Zugangsvoraussetzungen zu ihren Forschungsdaten.

(9) Erlaubt eine Daten-Partei die Nutzung von Forschungsdaten, hat die in der Genehmigung genannte GWAP-Partei den Forschenden – im Rahmen seiner Kapazitäten und seiner Zugangsregelungen - Zugang zu einem GWAP zur Nutzung der Daten zu gewähren. Den Zugang kann die GWAP-Partei nur aus technischen Gründen, bei Verstößen der Forschenden

gegen die Sicherheitskriterien zum Schutz der Forschungsdaten oder wenn die Zugangsregelungen bzw. Aufsichtsregelungen der GWAP-Partei nicht vorliegen verweigern.

(10) Die GWAP-Partei führt vor Nutzung des GWAP durch die Forschenden eine Identitätskontrolle (amtliches Ausweisdokument) durch und gewährleistet, dass alle Mindestsicherheitskriterien des GWAP umgesetzt sind. Es weist die Forschenden vor der ersten Nutzung auf die Regeln zur Arbeit in Datensicherheitsräumen hin und verpflichtet ihn zur Einhaltung der datenschutzrechtlichen Vertraulichkeit. Die Identitätskontrolle und Einweisung der Regelungen müssen durch die Unterschrift der Forschenden und einer Mitarbeiterin oder eines Mitarbeiters der GWAP-Partei auf dem Formular "Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes" (siehe Anhang 2) protokolliert werden, bevor Forschenden der Zugang gewährt wird.

(11) Die unterzeichneten Formulare "Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes" (siehe Anhang 2) sind von der GWAP-Partei zu archivieren. Eine Daten-Partei hat jederzeit Anspruch darauf, die unterzeichneten Formulare der Forschenden, die auf ihre Daten zugreifen, einzusehen.

(12) Jede GWAP-Partei ist für die Einhaltung der in der **Anlage 1** genannten technischen und organisatorischen Maßnahmen zum Schutz der Daten an den GWAP seiner Institution verantwortlich. Die in dieser Anlage beschriebenen Maßnahmen, die Bestandteil dieser Vereinbarung sind, können einvernehmlich ohne eine Änderung dieser Kooperationsvereinbarung geändert werden. Jede Änderung ist allerdings schriftlich zu dokumentieren und mit dem Datum der Änderung dieser Vereinbarung beizufügen.

(13) Jede Daten-Partei ist für die Sicherheit der Daten auf den eigenen Servern selbst verantwortlich.

(14) Bei Verstößen durch Forschende gegen die in Anlage 2 definierten Regelungen zur Nutzung von Gastwissenschaftsarbeitsplätzen oder anderweitigen Verstößen gegen die Datenschutzrichtlinien der jeweiligen Daten-Partei müssen sowohl die involvierte Daten-Partei als auch die GWAP-Partei über die Verstöße informiert werden. Die Entscheidung über Sanktionen gegenüber dem/der Forschenden obliegt der Partei, deren Daten kompromittiert wurden.

§ 5 Kosten

Jeder Kooperationspartner trägt die Kosten für die von ihm zu erbringenden Kooperationsbeiträge (§ 4) selbst. Eine Kostenerstattung findet nicht statt.

§ 6 Haftung

(1) Die Kooperationspartner werden für die Durchführung des Vorhabens die Zeit und die Sorgfalt aufwenden, die bei Berücksichtigung der anerkannten Regeln der Wissenschaft und Technik notwendig sind, um die hier definierten technischen- und organisatorischen Maßnahmen umzusetzen.

(2) Die Kooperationspartner werden in sachlich gebotenen Zeitabständen unter Beteiligung der mit dem Vorhaben befassten Mitarbeiterinnen und Mitarbeiter ein Kooperationsgespräch führen.

(3) Die Kooperationspartner benennen einander je eine Ansprechperson für alle im Rahmen der Kooperation abzustimmenden Angelegenheiten.

(4) In ihrem Innenverhältnis haften die Kooperationspartner für die Verletzung derjenigen Verpflichtungen, die sich aus der in diesem Vertrag geregelten Aufgabenverteilung (§ 4) ergeben. Insbesondere haften sie als GWAP-Partei für Verletzungen der datenschutzrechtlichen Verpflichtungen im Zusammenhang mit dem Zugang zu den GWAP und zu den Thin Clients (Zutritts- Zugangs-, Zugriffskontrolle usw.). Als Daten-Partei haften sie im Innenverhältnis insbesondere für die rechtswidrige Erhebung, Bearbeitung und Bereitstellung der Daten. Insbesondere die Prüfung der datenschutzrechtlichen Zulässigkeit der Datenbearbeitung fällt ausschließlich in den Verantwortungsbereich der Daten-Partei.

(5) Die Kooperationspartner stellen sich wechselseitig von Ansprüchen frei, mit denen sie aus der Verletzung von Pflichten in Anspruch genommen werden, die nach der in dieser Vereinbarung geregelten Aufgabenverteilung von einem der anderen Kooperationspartner zu erfüllen sind.

§ 7 Laufzeit der Vereinbarung und Kündigung

(1) Die Vereinbarung tritt am _____ in Kraft und wird zunächst bis _____ befristet.

(2) Die Vereinbarung kann von einem Kooperationspartner vorzeitig nur aus wichtigem Grund gekündigt werden z.B. wenn finanzielle, technische oder organisatorische Gründe die Umsetzung der technischen und organisatorischen Maßnahmen (Anhang 1) nicht mehr gestatten. Die Kündigung bedarf der Schriftform und ist gegenüber sämtlichen Kooperationspartnern zu erklären ist,

(3) Zudem haben die Kooperationspartner das Recht, die Vereinbarung gegenüber einem bestimmten Vertragspartner aus wichtigem Grund einvernehmlich fristlos zu kündigen. Vor der Kündigung ist dem zu kündigenden Kooperationspartner Gelegenheit zur Stellungnahme bzw. zum Ausräumen des Kündigungsgrundes zu geben. Die Kündigung bedarf der Schriftform und ist von allen Vertragspartnern – bis auf den, der gekündigt werden soll - zu unterzeichnen.

(4) Wichtige Gründe im Sinne der Absätze 2 und 3 sind insbesondere, aber nicht nur Verstöße eines Kooperationspartners gegen die in Anlage 1 vereinbarten Maßnahmen zum Schutz der Forschungsdaten.

(5) Im Falle einer Kündigung nach den Absätzen 2 und 3 wird die Zusammenarbeit von den übrigen Kooperationspartnern fortgeführt.

§ 8 Weitere Bestimmungen

(1) Die Kooperationspartner gründen mit ihrer Zusammenarbeit keine Gesellschaft, die nach außen am Rechtsverkehr teilnimmt. Sie sind allein auf Grundlage dieser Vereinbarung nicht berechtigt, die jeweils anderen Kooperationspartner aktiv oder passiv zu vertreten.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so bleibt die Gültigkeit der übrigen Bestimmungen davon unberührt. Die Vertragspartner werden sich in einem solchen Fall in gegenseitigem Einvernehmen um eine Vertragsergänzung im Sinne des ursprünglich Gewollten bemühen.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Änderung der Schriftformklausel.

_____, den _____

_____, den _____

_____, den _____

Anlage 1: Technische und organisatorische Maßnahmen zum Schutz der gastwissenschaftlichen Arbeitsplätze

Anlage 2: Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes

Anlage 1:

Technische und organisatorische Maßnahmen zum Schutz der gastwissenschaftlichen Arbeitsplätze

Ein GWAP innerhalb des RDCnet definiert sich als dedizierter Arbeitsplatz für Forschenden an dem sensible Daten externer Institutionen zugänglich gemacht werden können. Ein GWAP befindet sich in einer gegen unbefugten Zugriff geschützten Räumlichkeit (Datensicherheitsraum) und verfügt über eine Hard- und Softwareausstattung, welche den sicheren „Remote Access“ zu Servern der Daten-Partei ermöglicht. Um dies zu gewährleisten, werden im Folgenden technische und organisatorische Maßnahmen definiert, die jeder Kooperationspartner für die Akkreditierung eines sicheren GWAP innerhalb es RDCnet erfüllen muss.

(1) Raumsicherung

Die im RDCnet bereitgestellten GWAP müssen sich, zum Zeitpunkt der Nutzung durch Forschenden, in kontrollierten Datensicherheitsräumen befinden (wird der GWAP nicht genutzt, kann auch die Räumlichkeit für andere Zwecke verwendet werden). Die GWAP-Partei muss gewährleisten, dass der Datensicherheitsraum während der Nutzung eines GWAP durch Forschende durch die folgenden Maßnahmen geschützt ist:

(1.1) Vor Zutritt zum Datensicherheitsraum muss die Identität der Forschenden durch einen amtlichen Lichtbildausweis überprüft werden. Zudem müssen sie auf die im Datensicherheitsraum und am GWAP geltenden Sicherheitsregelungen hingewiesen werden. Diese Einweisung und die Identitätskontrolle sind durch die Unterschriften eines/r FDZ-Mitarbeiters/in der GWAP-Partei und der Forschenden auf dem Formular „Regelung zur Nutzung von Gastwissenschaftsarbeitsplätzen innerhalb eines Datensicherheitsraumes“ (siehe Anhang 2) zu protokollieren und zu bestätigen.

(1.2) Bei erfolgreicher Identitätskontrolle kann den Forschenden ein Schlüssel oder eine Zugangskarte zum weiteren Betreten des Datensicherheitsraumes für die im Nutzungsantrag festgelegte Zeit ausgehändigt werden. Optional kann der Einlass auch manuell durch Fachpersonal der GWAP-Partei erfolgen.

(1.3) Der Datensicherheitsraum muss bei Nichtnutzung stets verschlossen sein und kann von den Forschenden nur durch den ausgehändigten Schlüssel/Zugangskarten oder manuellen Einlass durch Fachpersonal der GWAP-Partei betreten werden. Die anzuwendende Sicherheitsmechanik kann durch die GWAP-Partei selbst gewählt werden, muss jedoch gewährleisten, dass der Datensicherheitsraum nur für Fachpersonal der GWAP-Partei (mit entsprechender Berechtigung) und für Forschenden mit denen ausgehändigten Schlüssel/Zugangskarten zugänglich ist.

(1.4) Die Mitnahme von eigenen PCs (Laptop, Tablets), Mobiltelefonen, Geräten zur Bildaufnahme oder Massenspeichergeräten an den GWAP ist den Forschenden untersagt. Den Forschenden müssen deshalb Schließfächer oder Spinde zur Verfügung stehen, um persönliche Gegenstände sicher zu lagern.

(1.5) Der Datensicherheitsraum muss regelmäßig auf Fremdzugang und der Einhaltung von Punkt 1.4 kontrolliert werden. Alternative Umsetzungsmöglichkeiten:

- i. Physische Sichtung durch Mitarbeitende der GWAP-Partei.
- ii. Nutzung von Überwachungskameras (*Hierfür werden zusätzlich benötigt: vollständiges Informationsblatt (Aushang) und vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung*)

(1.6) Der Datensicherheitsraum darf ausschließlich innerhalb der regulären Öffnungszeiten der GWAP-Partei durch Forschenden betreten werden. Am Ende eines jeden Arbeitstages muss kontrolliert werden, dass sich niemand im Datensicherheitsraum befindet und dieser entsprechende abgeschlossen ist.

(1.7) Innerhalb des Datensicherheitsraum muss gewährleistet sein, dass der Bildschirm nur von den jeweilig autorisierten Forschenden und nicht von unbefugten Personen einsehbar ist. Möglichkeiten zur Umsetzung:

- i. Aufstellen von Trennwänden oder Sichtschutz.
- ii. Positionierung der Arbeitsplätze und Nutzung von Blickschutzfilter für Monitore, sodass die Einsicht auf andere Bildschirme innerhalb des Datensicherheitsraumes nicht ohne weiteres möglich ist.

(1.8) Fachpersonal der GWAP-Partei, das den Forschenden für Supportanfragen vor Ort bereitsteht (und somit bei technischer Hilfestellung den Bildschirm einsehen kann), muss im Rahmen seiner Anstellung auf den Datenschutz verpflichtet sein.

(1.9) Für die Bearbeitung von qualitativen Daten die Audiospuren beinhalten (z.B. Interviews), müssen den Forschenden Kopfhörer bereitgestellt werden.

(2) Technische Kriterien:

Als Analyse Computer der GWAP werden Thin Clients genutzt. Ein solcher Client dient lediglich als Verbindung (über die Tastatur, die Computermouse und den Bildschirm) zwischen dem Arbeitsplatz der GWAP-Partei und der bereitgestellten virtuellen Umgebung auf dem Server der Daten-Partei. Die Daten verlassen also zu keinem Zeitpunkt die Server der Daten-Partei und der Zugriff erfolgt remote über eine kryptographisch gesicherte Verbindung, die dem aktuellen Stand der Technik entspricht. Um dies zu gewährleisten, umfasst die Konfiguration des Thin Clients folgende Aspekte:

- i. Installation und Konfiguration eines Betriebssystems, das die Implementierung der „VMware Horizon Client“ Software ermöglicht. Zudem muss die Software regelmäßig aktualisiert und Sicherheitspatches zeitnah installiert werden.
- ii. Die Möglichkeit zum Kopieren, Speichern, Versenden, Bildschirmaufnahmen oder der Nutzung von USB-Schnittstellen muss ausgeschlossen sein.
- iii. Implementierung einer Netzwerkstruktur, die sicherstellt, dass der Zugang ausschließlich über gesicherte Verbindungen zu legitimen Servern innerhalb des RDCnet möglich ist.
- iv. Installation und Konfiguration der Remote Access Software „VMware Horizon Client“, um auf die virtuelle Umgebung des Zielservers zuzugreifen.
- v. Der Thin-Client muss gegenüber dem internen Netzwerk der Institution abgesichert sein.
- vi. Einigen sich die Kooperationspartner gemäß §4 Abs. 6 auf die Verwendung einer anderen Remote-Access-Software als VMware Horizon, so muss diese Software ebenfalls auf den Thin-Clients installiert und konfiguriert werden.

Anlage 2: Regelung zur Nutzung von Gastwissenschaftsarbetsplätzen innerhalb eines Datensicherheitsraumes

GWAP wird durch folgende Institution bereitgestellt: <input type="text"/>	Name Forschende*r: <input type="text"/>
Name Mitarbeitende*r der GWAP stellenden Institution: <input type="text"/>	Datum: <input type="text"/>

Für die Nutzung eines über das RDCnet gebuchten Gastwissenschaftsarbetsplatz (GWAP) gelten innerhalb des Datensicherheitsraumes und am zur Verfügung gestellten Arbeitsplatz folgende Regelungen zum Schutz der Forschungsdaten:

- I. Der Datensicherheitsraum darf ausschließlich von autorisierten Personen betreten werden. Den Forschenden ist es untersagt, anderen Personen Zutritt zum Datensicherheitsraum zu gewähren.
- II. Die Mitnahme von eigenen PCs (Laptop, Tablets), Mobiltelefonen, Geräten zur Bildaufnahme oder Massenspeichergeräten innerhalb des Datensicherheitsraumes ist den Forschenden untersagt.
- III. Der Datensicherheitsraum darf ausschließlich während der regulären Öffnungszeiten der Institution, die das GWAP bereitstellt, von den Forschenden betreten werden.
- IV. Jeder Versuch, die Forschungsdaten auf irgendeine Weise außerhalb des Datensicherheitsraumes zugänglich zu machen oder anderen Personen innerhalb des Datensicherheitsraumes Zugang zu den Daten zu gewähren, ist untersagt.

Der Datensicherheitsraum wird in regelmäßigen Abständen durch das Personal der GWAP bereitstellenden Institution auf die Einhaltung der oben genannten Regelungen kontrolliert. Ein Verstoß führt zu einem sofortigen Ausschluss von der Nutzung der GWAP aller im RDCnet teilnehmenden Institutionen. Zudem werden alle involvierten Parteien über den Verstoß informiert.

Mit der Unterzeichnung dieses Formulars bestätigt die Mitarbeitende oder der Mitarbeitende der GWAP bereitstellenden Institution, dass sie oder er die oben genannte Forschende oder den oben genannten Forschenden auf die Regelung zur Nutzung von Gastwissenschaftsarbetsplätzen innerhalb eines Datensicherheitsraumes hingewiesen und die Identität mittels eines Lichtbildausweises überprüft hat. Die oder der Forschende bestätigt mit der Unterzeichnung des Formulars die Einhaltung der angegebenen Regelungen und die Zukentnissnahme der Konsequenzen bei Verstößen.

Unterschrift Mitarbeitende*r

Unterschrift Forschende*r

Literaturverzeichnis

Adena, Maja, Aßmann, Christian, Bambey, Doris, Blask, Katarina, Blätte, Andreas, Bosnjak, Michael, Buck, Daniel, Bug, Mathias, Busch, Anja, Fräßdorf, Anna, Fuß, Daniel, Goebel, Jan, Hollstein, Betina, Jungbauer-Gans, Monika, Kern, Dagmar, Klas, Claus-Peter, Kretzer, Susanne, Liebig, Stefan, Mayer-Ahuja, Nicole, ... Zindler, Susanne. (2020). *Consortium for the Social, Behavioural, Educational, and Economic Sciences (KonsortSWD) (This version reflects revisions to the proposal to adjust to the amount of funding approved)*. Zenodo.

<https://doi.org/10.5281/zenodo.4446457>

Matthew Woollard, Beate Lichtwardt, Elizabeth Lea Bishop, & Dana Müller. (2021). *D5.9 Framework and contract for international data use agreements on remote access to confidential data (v1.0)*. Zenodo. <https://doi.org/10.5281/zenodo.4534286>

Schallaböck, Jan, Hoffstätter, Ute, Buck, Daniel, & Linne, Monika. (2022). *Mustervertrag Datennutzung KonsortSWD (1.0.0)*. Zenodo. <https://doi.org/10.5281/zenodo.5828114>

Schiller, David H., Eberle, Johanna, Fuß, Daniel, Goebel, Jan, Heining, Jörg, Mika, Tatjana et al. (2017): *Standards des sicheren Datenzugangs in den Sozial- und Wirtschaftswissenschaften. Rat für Sozial- und Wirtschaftsdaten (RatSWD) (RatSWD Working Paper, 261/2017)*.

Impressum

Kontakt:

Neil Murray

German Institute for Economic Research (DIW)

Mohrenstrasse 58

10117 Berlin, Germany

nmurray@diw.de

Tel.: +49 30 89789 – 326

Berlin, Oktober 2024

KonsortSWD Working Paper:

KonsortSWD baut als Teil der Nationalen Forschungsdateninfrastruktur Angebote zur Unterstützung von Forschung mit Daten in den Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften auf. Unsere Mission ist es, die Forschungsdateninfrastruktur zur Beforschung der Gesellschaft zu stärken, zu erweitern und zu vertiefen. Sie soll nutzungsorientiert ausgestaltet sein und die Bedürfnisse der Forschungscommunities berücksichtigen. Wichtiger Grundstein ist dabei das seit über zwei Jahrzehnten durch den Rat für Sozial- und Wirtschaftsdaten (RatSWD) aufgebaute Netzwerk von Forschungsdatenzentren.

In dieser Reihe erscheinen Beiträge rund um das Forschungsdatenmanagement, die im Kontext von KonsortSWD entstehen. Beiträge, die extern und doppelblind begutachtet wurden sind entsprechend gekennzeichnet.

KonsortSWD wird im Rahmen der NFDI durch die Deutsche Forschungsgemeinschaft (DFG) gefördert – Projektnummer: 442494171.



Diese Veröffentlichung ist unter der Creative-Commons-Lizenz (CC BY 4.0) lizenziert:

<https://creativecommons.org/licenses/by/4.0/>

doi: [10.5281/zenodo.13827792](https://doi.org/10.5281/zenodo.13827792)

Zitationsvorschlag:

Murray, N., Goebel, J. (2024). *Vertragliche Grundlagen zur Teilnahme am RDCnet (v. 2.0)*, KonsortSWD Working Paper 1/2024. Berlin. Deutsches Institut für Wirtschaftsforschung (DIW). <https://doi.org/10.5281/zenodo.13827792>