SOEP The Socio-Economic Panel

SOEP | Datenschutzverfahren

Verfahren für den Datenschutz beim Zugang zu den SOEP-Daten innerhalb und außerhalb des DIW Berlin

Berlin, Mai 2020

DIW SOEP

SOEP | Datenschutzverfahren

Verfahren für den Datenschutz bei der Verarbeitung der in den Erhebungen des Sozio-oekonomischen Panel (SOEP) bei den Teilnehmerinnen und Teilnehmern an der Studie „Leben in Deutschland“ gewonnenen Daten und bei deren Zugänglichmachung innerhalb und außerhalb des DIW Berlin.

Berlin, Mai 2020

Inhaltsverzeichnis

1. Grundlegende Datenschutzprinzipien

1.1. Das SOEP am DIW Berlin

Als am DIW Berlin beheimatete forschungsbasierte Infrastruktureinrichtung unterliegt die forschungsbasierte Infrastruktureinrichtung SOEP den für das DIW Berlin geltenden gesetzlichen Datenschutzregeln sowie denen, die sich das DIW in seiner Datenschutzleitlinie und seinem Datenschutzkonzept gegeben hat. Das SOEP ist in die datenschutzrechtlichen Strukturen und Verfahren des DIW Berlin eingebunden. So liegt die datenschutzrechtliche Gesamtverantwortung für das SOEP beim Vorstand des DIW Berlin. Die Beschäftigten und Stipendiaten des SOEP werden nach den für sämtliche Mitarbeiterinnen und Mitarbeiter geltenden Regeln auf die Befolgung des Datenschutzes verpflichtet und in die entsprechenden Bestimmungen eingewiesen. Der betriebliche Datenschutzbeauftragte und die Stabstelle Datenschutz des DIW Berlin stehen dem SOEP und seinen Beschäftigten in gleicher Weise zur Verfügung wie den übrigen am DIW Berlin Tätigen.

Die im Rahmen seines Forschungsauftrags vom SOEP seit 1984 durchgeführte sozialwissenschaftliche Längsschnittstudie „Leben in Deutschland“ und die dabei von den Teilnehmerinnen und Teilnehmern an dieser Studie erhobenen Daten erfordern aber spezifische Regeln zum Schutz ihrer Grundrechte und Freiheiten. Diese sind in diesem Dokument beschrieben und für das Handeln des SOEP, seiner Beschäftigten, Stipendiaten und seiner Gäste sowie sämtlicher Forschenden, die mit diesen Daten arbeiten, verbindlich.

1.2. Gemeinsame datenschutzrechtliche Verantwortung mit Umfrageunternehmen und Kooperationspartnern

Im Zusammenhang mit der Studie „Leben in Deutschland“ nimmt das DIW Berlin seine datenschutzrechtliche Verantwortung gemeinsam mit dem mit der Befragung der Teilnehmerinnen und Teilnehmer beauftragten Umfrageunternehmen wahr. Das DIW Berlin schließt mit dem Umfrageunternehmen deshalb einen Vertrag nach Art 26 DSGVO. Einen solchen Vertrag schließt es – abhängig von der konkreten Ausgestaltung der Kooperation – auch mit wissenschaftlichen Kooperationspartnern, die im Rahmen eines Forschungsprojekts in die Datenerhebung mit eingebunden sind.

1.3. Trennungsprinzip

Grundlage des Schutzes der Daten der Studienteilnehmerinnen und -teilnehmer ist die strikte Einhaltung des Trennungsprinzips dergestalt, dass ihre Kontaktdaten streng getrennt von den Befragungsdaten gespeichert und aufbewahrt werden. Die personenbezogenen Kontaktdaten befinden sich ausschließ-

lich bei dem beauftragten Umfrageunternehmen. Niemand im DIW Berlin, auch nicht im SOEP kennt die Kontaktdaten und hat zu ihnen Zugang. Das SOEP erhält vom Befragungsunternehmen ausschließlich die Befragungsdaten aus den einzelnen Erhebungen der Studie. Dieses Trennungsprinzip ist auch vertraglich im Verhältnis zu dem Umfrageunternehmen verankert. Das SOEP wird es auch bei einem Wechsel des Dienstleisters beachten und hat auch dafür die vertraglichen Voraussetzungen geschaffen.

Obwohl das SOEP vom Umfrageunternehmen also regelmäßig faktisch anonymisierte Daten erhält, die als solche dem Schutz der datenschutzrechtlicher Bestimmungen grundsätzlich nicht unterfallen, unterwirft sie das SOEP den für personenbezogene Daten geltenden gesetzlichen und den in diesem Dokument beschriebenen Regeln und wendet sie zum Schutz der Teilnehmerinnen und Teilnehmer an der Studie darauf an.

1.4. Einwilligungsbasierte Datenverarbeitung

Die Befragungen der an der Studie „Leben in Deutschland“ Teilnehmenden und die weitere Verarbeitung der Daten sind einwilligungsbasiert. Die Teilnehmerinnen und Teilnehmer werden vor der Befragung und vor Abgabe ihrer Einwilligungserklärung umfassend informiert, insbesondere – aber nicht nur - über die Zwecke und den Umfang der Datenerhebung sowie über den Kreis der zu den Daten Zugangsberechtigten. Vor der Befragung werden sie außerdem über ihre Datenschutzrechte aufgeklärt.

1.5. Einschränkung der Zugangsberechtigung

Die IT-Struktur des SOEP ist von der des übrigen DIW Berlin abgeschottet. Das SOEP betreibt eigene zentrale Server und Netzlaufwerke, auf die Beschäftigte anderer Abteilungen, auch der anderen wissenschaftlichen Abteilungen keinen generellen Zugang haben. Wissenschaftlerinnen und Wissenschaftler des DIW Berlin erhalten ihn ausschließlich auf Grundlage einer gesonderten Erlaubnis zu wissenschaftlichen Zwecken.

Auch innerhalb des SOEP ist der Zugang zu den Befragungsdaten der Studie „Leben in Deutschland“ durch ein gestaffeltes System an Zugangsberechtigungen reglementiert (siehe Übersicht in Tabelle 1).

Externen Forschenden stellt das DIW Berlin die Datensätze der Studie „Leben in Deutschland“ über sein Forschungsdatenzentrum ausschließlich auf Grundlage von Datenweitergabeverträgen - Forschenden aus Gebieten außerhalb des Europäischen Wirtschaftsraums unter Einbeziehung der EU-Standardvertragsklauseln – zur Verfügung.

Besondere Regelungen gelten für Gastwissenschaftlerinnen und Gastwissenschaftler, die am SOEP mit den SOEP-Datensätzen forschen (vgl. 3.2.1).

2. Überblick

Tabelle 1 stellt synoptisch die Zugangsvoraussetzungen für die diversen Nutzergruppen zu den unterschiedlichen SOEP-Datenbeständen bzw. den Erweiterungen um Regionaldaten dar.

Tabelle 1:

Übersicht über die Zugangsregeln der unterschiedlichen Nutzergruppen zu den Datenbeständen des SOEP

(Stand: 02.02.2010)

	Abt. SOEP	DIW Berlin	Externe WissenschaftlerInnen in der Abt. SOEP	Externe Wissenschaftler-Innen mit DWV
Namen und Adressen der SOEP-Befragten	-/-	-/-	-/-	-/-
SOEP-Rohdaten	AV + DSV + eingeschränkter Benutzerkreis	-/-	-/-	-/-
SOEP-Standard (SUF)	AV + DSV	AV + DSV	DWV + DSV	DWV + lokale DSV
Zusätzliche Gebietstypisierungen (Gemeindegrößenklassen und BIK-Regionen)	AV + DSV	AV + DSV	DWV + DSV	DWV + ZV 1 + DSK
Raumordnungsregionen	AV + DSV	AV + DSV	DWV + DSV	DWV + ZV 2 + DSK
Kreise	AV + DSV	AV + DSV	DWV + DSV + SOEPonsite mit protokolliertem Zugriff	DWV + ZV 3 per SOEPremote execution
Postleitzahlen	AV + DSV	AV + DSV + SOEPonsite mit protokolliertem Zugriff	DWV + DSV + SOEPonsite mit protokolliertem Zugriff	-/-
Microm Zusatzdaten	AV + DSV	AV + DSV	DWV + DSV + SOEPonsite mit protokolliertem Zugriff	-/-
Klartextangaben	AV + DSV + Nutzung auf Anfrage	-/-	DWV + DSV + SOEPonsite mit protokolliertem Zugriff	-/-

Geo-Koordinaten	AV + DSV + stark eingeschränkter Benutzerkreis	AV + DSV + SOEPonsite mit protokolliertem Zugriff und getrennter Datenhaltung von Koordinate und Befragungsdaten	DWV + DSV + SOEPonsite mit protokolliertem Zugriff und getrennter Datenhaltung von Koordinate und Befragungsdaten	-/-
Archiv für Re-Analysen	AV + DSV + ggf. eingeschränkter Benutzerkreis	AV + DSV + ggf. weitere Maßnahmen[1)]	AV + DSV + ggf. weitere Maßnahmen[1)]	DWV + lokale DSV + ggf. ZV[1)]

AV = Arbeitsvertrag;
DSV = Datenschutzverpflichtung;
DWV = Datennutzungsvertrag;
ZV = Zusatzvertrag;
DSK = vom DIW Berlin geprüftes Datenschutzkonzept
SOEPonsite = Nutzung in den Räumen des SOEP mit zusätzlicher Verpflichtung
-/- = Kein Zugriff erlaubt

1) Welche Einschränkungen greifen, hängt von der Art der archivierten Daten ab.

3. Aufbereitung und Nutzung der SOEP Daten im SOEP

Die Kontaktdaten der befragten Personen werden nach der Befragung noch beim Erhebungsdienstleister von den Befragungsdaten getrennt und bleiben ausschließlich beim Erhebungsinstitut.

Zur weiteren Bearbeitung und Aufbereitung am DIW Berlin erhält das SOEP ausschließlich die Befragungsdaten, und zwar mittels einer verschlüsselten Verbindung. Die Übermittlung erfolgt ausschließlich an die dazu legitimierten Beschäftigten des SOEP. Geo-Koordinaten werden getrennt von den Befragungsdaten sowie ebenfalls ausschließlich in verschlüsselten Dateien an das SOEP übermittelt.

Alle personenbeziehbaren Angaben aus den laufenden Erhebungen werden durch die Verwendung von systemfreien Personen- und Haushalts-IDs anonymisiert an das DIW Berlin ausgeliefert. Auf diese Weise erhält das DIW Berlin ausschließlich faktisch anonymisierte Daten.

3.1. Aufbereitung der SOEP-Rohdaten im FDZ SOEP

Die vom Erhebungsinstitut beim SOEP eingehenden Daten (SOEP-Rohdaten) werden im FDZ SOEP auf einem gesonderten Laufwerk gespeichert, zu der nur die unmittelbar verantwortlichen Mitarbeiterinnen und Mitarbeiter des SOEP Zugang haben. Ausschließlich diesen ist es vorbehalten, die Daten Jahres übergreifend zusammenzuführen und an Hand von Vornamen, Geschlecht und Geburtsdatum die korrekte zeitliche Verknüpfung zu kontrollieren.

Die SOEP-Rohdaten unterliegen zudem einem besonderen Zugangsschutz. Jeder Computer, von dem aus Rohdaten gespeichert werden, ist nur mit einer personalisierten Nutzerkennung und mit einer Passwort-Kombination benutzbar. Bei Nicht-Benutzung (Idle) über mehrere Minuten wird das Passwort automatisch neu erfragt.

Bei der Aufbereitung dieser SOEP-Rohdaten für die standardmäßige wissenschaftliche Weiternutzung werden als weitere Datenschutzmaßnahmen Klartextangaben[1] sowie alle über das Bundesland hinausgehenden regional differenzierenden Merkmale gelöscht. Diese Datensätze, sind Basis für die weitere nutzerfreundliche Aufbereitung der SOEP-Daten, die anschließend per individuell verschlüsselter Übertragung im Rahmen der Datenweitergabe an vertraglich und datenschutzrechtlich verpflichtete Nutzende gehen (die so genannten „Scientific Use Files“ (SOEP-SUF-Daten), siehe Abschnitt 3.2).

3.2. Nutzung der SOEP-SUF-Daten und der Regionaldaten im SOEP und im übrigen DIW Berlin

3.2.1. SOEP-SUF-Daten

Nach der Prüfung und Aufbereitung sowie der Durchführung der datenschutzrelevanten Maßnahmen werden die SOEP-SUF-Daten für die standardmäßige wissenschaftliche Nutzung vom FDZ SOEP auf einem gesonderten Netzlaufwerk für die Datenweitergabe und für inhaltliche Analysen bereitgestellt. Auf das Netzlaufwerk mit diesen zur Weitergabe freigegebenen SOEP-SUF-Daten können auch Beschäftigte des DIW Berlin erst nach Einrichten einer persönlichen Nutzer-kennung mit individuellem Passwort und der Verpflichtung zur Einhaltung datenschutzrechtlicher Nutzungsbestimmungen zugreifen. Die Freigabe des Zugangs erfolgt durch das FDZ SOEP.

Dies gilt auch für Gäste des SOEP, sofern sie nicht auf erweiterte Regionaldaten zugreifen wollen. Diesen wird nach Unterzeichnung der Datenschutzerklärung eine Gastkennung für den Datenzugang eingerichtet wird.

1 Klartextangaben umfassen Berufs- und Bildungsbezeichnungen und weitere offene Angaben der Interviewten sowie Vornamen.

Alle am DIW Berlin forschenden Gäste des SOEP sind einer/einem Beschäftigten des SOEP (Betreuerin/Betreuer) zugeordnet. Dieser Betreuer bzw. diese Betreuerin füllt den Antrag auf eine Nutzerkennung aus und bestätigt mit ihrer/seiner Unterschrift die Notwendigkeit der verschiedenen Datenzugänge. Administriert werden die Nutzerkennungen für die Gäste - wie auch für die Beschäftigten des DIW Berlin - zentral von der Stabsabteilung Informationstechnik (IT). Auch Gäste werden wie Mitarbeiterinnen und Mitarbeiter des DIW Berlin datenschutzrechtlich verpflichtet (siehe Anhang B.1.a).

Ein Zugang zu den SOEP-Daten besteht daher im DIW Berlin für Mitarbeiterinnen und Mitarbeiter wie für Gäste (Praktikantinnen und Praktikanten, Gastforscherinnen und Gastforscher) nur unter der Bedingung einer personalisiert freigeschalteten Nutzerkennung und Passwortkombination sowie der persönlichen Verpflichtung auf den Datenschutz.

Alle weitergehenden Nutzungen der SOEP-Daten – wie etwa die Nutzung von Klartextangaben, tiefer gegliederten Regionalmerkmalen oder auch die Verknüpfung mit anderen Datensätzen durch spezifische, datenschutzrechtlich anerkannte Verfahren des „Statistical Matching“ können nur nach Absprache mit der Leitung des FDZ SOEP erfolgen und unterliegen jeweils weitergehenden personenbezogenen Datenschutzverpflichtungen und ggf. zusätzlichen technisch-organisatorischen Maßnahmen. Direkte Verknüpfungen personenbezogener Daten der Befragungspersonen aus dem SOEP mit ihren Daten aus anderen Datenbeständen oder Registern („Record Linkage“) führt das SOEP ausschließlich nach einer ausdrücklich erteilten Einwilligung der befragten Personen, die von ihnen für jedes beabsichtigte „Record Linkage“ gesondert eingeholt wird, durch. Die dafür notwendigen eindeutigen Schlüsselmerkmale (wie z.B. Name, Geburtsdatum oder Sozialversicherungsnummer, etc.) werden vom Erhebungsinstitut nach Einwilligung getrennt erhoben und direkt an den jeweiligen Kooperationspartner (z.B. Forschungsdatenzentrum der Rentenversicherung) übermittelt. Eine Verbindung mit diesen externen Daten (zum Beispiel zum Rentenbezug) ist im Folgenden nur über anonymisierte Identifikatoren möglich. Die eindeutigen Schlüsselmerkmale wie Sozialversicherungsnummer werden zu keinem Zeitpunkt an das SOEP übermittelt und vom Kooperationspartner nach Aufbereitung der anonymisierten Daten gelöscht.

3.2.2. Regionaldaten

Die Nutzung zusätzlicher Regionalinformationen (Landkreise und kreisfreie Städte, Gemeindekennziffern, Postleitzahlen, Hauskoordinaten) ist ausschließlich von Servern des DIW Berlin aus möglich, und zwar regelmäßig nur von innerhalb der Büroräume des DIW Berlin. Zugänglich sind diese Daten zudem nur Personen, denen das SOEP eine gesonderte Berechtigung dazu erteilt hat. Erlaubt das DIW – ausschließlich seinen Beschäftigten,- nicht seinen Gästen – im Einzelfall den Zugang zu diesen Daten von außerhalb der Büroräume des DIW, stellt es durch Dienstanweisungen an die Beschäftigten sicher, dass die Daten nicht auf ihre lokalen Rechner, auf mobile Datenträger oder anderweitig kopiert und übertragen werden und dass sie durch technische und organisatorische Maßnahmen vor einer Kenntnisnahme durch Dritte geschützt werden.

Der Zugriff auf die Koordinaten ist auch für Beschäftigte des DIW Berlin nicht in Verbindung mit den Befragungsdaten möglich. Vielmehr erfolgt der Zugriff über die gleichen Server wie für externe Gäste (siehe Kapitel 4.3.2). Beschäftigten des DIW Berlin ist es jedoch möglich, auf diese beiden Server von ihren Arbeitsplatzrechnern aus zuzugreifen.

4. Zugang zu SOEP-Daten für DIW-Externe

4.1. Übermittelung als Scientific Use File

Die Nutzung der anonymisierten SOEP-Daten außerhalb des DIW Berlin erfolgt nur für wissenschaftliche Zwecke auf der Grundlage eines Datenweitergabevertrages der antragstellenden Forschungsinstitution. Enthalten die Datensätze Informationen, die auf Grundlage genetischer Analysen generiert wurden, stellt sie das DIW Berlin zudem nur für Forschungsprojekte zur Verfügung, deren wissenschaftsethische Vertretbarkeit durch das positive Votum einer Ethikkommission bescheinigt ist.

Der Datenweitergabevertrag enthält neben der institutionellen Anbindung auch eine zeitliche Befristung, die Angabe des Forschungszwecks sowie die Verpflichtung zur Einhaltung datenschutzrechtlicher Maßnahmen am Ort der Nutzung.

Erst nach Abschluss dieses Vertrages werden die SOEP-SUF-Daten per individuellem Downloadlink verschlüsselt ausgeliefert. Nutzer außerhalb des EWR-Raums (EU, Schweiz, Norwegen und Liechtenstein) erhalten nur Zugang nach einer vertraglichen Verpflichtung auf die EU-Standardvertragsklauseln und haben zudem nur Zugang zu einer 95%-Zufallsstichprobe der jeweils samplespezifischen ersten Welle des kompletten SOEP-Datenbestandes.

Die Nutzung von Gemeindegrößenklassen, BIK-Regionen oder Regionalinformationen auf der Ebene der Raumordnungsregionen außerhalb des DIW Berlin ist nur nach Vorlage eines erweiterten Datenschutzkonzeptes und dessen Prüfung durch die Stabstelle Datenschutz und/oder den Datenschutzbeauftragten des DIW Berlin innerhalb des EWR-Raums möglich.

Externe Nutzer, die mit tiefergegliederten Regionalinformationen arbeiten wollen, müssen entweder SOEPremote-execution (zurzeit nur für Kreiskennziffern möglich) nutzen oder als Gäste an das FDZ SOEP kommen.

4.2. Kontrollierte Datenfernverarbeitung (SOEPremote-execution)

Damit auch jenen externen Wissenschaftlerinnen und Wissenschaftlern, denen es nicht möglich ist, direkt vor Ort am DIW Berlin zu sein, zumindest die Nutzung der Kreisdaten (ca. 400 Regionen in Deutschland) ermöglicht wird, gibt es zudem einen kontrollierten Datenfernverarbeitungszugang (SOEPremote-execution): Nach Unterzeichnung und Prüfung eines zusätzlichen Datenschutzvertrages können Wissenschaftlernnen und Wissenschaftler ihre Auswertungssyntax an eine definierte E-Mail-Adresse am DIW Berlin senden und bekommen die auf Einhaltung des Daten-schutzes kontrollierten Ergebnisse wieder zurück gesendet. Bei diesem international bewährten Ver-fahren haben die Forschenden zu keiner Zeit außerhalb des DIW Berlin direkten Zugriff auf die Mikro-daten. Diese werden zu keinem Zeitpunkt außerhalb des DIW Berlin verarbeitet.

4.3. On-Site Zugriff

4.3.1. Nutzung von kleinräumigen Regionaldaten

Gastwissenschaftlerinnen und Gastwissenschaftler können am FDZ SOEP an speziell gesicherten Thin Clients in einem zugangskontrollierten Raum mit den SOEP Daten in Verbindung mit kleinräumigen Regionalinformationen arbeiten. An diesen Thin Clients besteht abgesehen von Tastatur, Maus und Bildschirm keine weitere Möglichkeit der Datenein- oder -ausgabe (z.B. USB-Anschluss oder Drucker). Von diesen Thin Clients kann jeweils eine verschlüsselte Verbindung zum Gästeserver aufgebaut werden, auf dem sich die Gäste mit einem persönlichen Account und Passwort anmelden. Alle Zugriffe und die Nutzung des Servers werden protokolliert. Neben der Nutzung von Regionalindikatoren auf der Basis von administrativen Einheiten und Postleitzahlen, haben die Nutzer auch die Möglichkeit, auf diesem Server die von ihnen mit Hilfe der Geo-Koordinaten generierten Indikatoren zu nutzen. Die Erstellung dieser Indikatoren wird im folgenden Kapitel 4.3.2 beschrieben.

Da die Thin Clients über keine Schnittstellen zum Import oder Export von Daten verfügen, werden alle Im- und Exports von FDZ Mitarbeitern durchgeführt und jeweils individuell datenschutzrechtlich geprüft. Datensätze auf der Ebene von Haushalten oder Personen dürfen nicht exportiert werden. Exportiert werden dürfen lediglich aggregierte Ergebnisse oder Grafiken.

4.3.2. Nutzung von Geo-Koordinaten

Für eine Nutzung der Hauskoordinaten wurde eine spezielle Serverumgebung innerhalb der IT des DIW Berlin aufgebaut („SOEPgeo“), die sicherstellt, dass keine Nutzerin und kein Nutzer dieser Daten zugleich Zugang zu diesen Hauskoordinaten und zu den Befragungsdaten haben. Auf diese Weise ist sichergestellt, dass selbst analysierenden Wissenschaftlerinnen oder Wissenschaftler nicht auf den Verknüpfungsalgorithmus zugreifen können. Grundlage des Konzepts ist es, dass während allen von Nutzerinnen und Nutzern ausgeführten Analysen die Geo-Koordinaten der SOEP-Haushalte von den Erhebungsinformationen getrennt gehalten werden. Zur Erzeugung von inhaltlichen Indikatoren innerhalb eines Geo-Informationsystems (GIS) oder innerhalb des Statistik Pakets R sind nur die Koordinaten ohne weitere Informationen über den Haushalt oder Personen in diesem Haushalt notwendig. Ein Zuspielen der durch die Nutzer in einem GIS erzeugten Indikatoren erfolgt durch Beschäftigte des FDZ SOEP. Die Nutzerinnen und Nutzer haben keinerlei Möglichkeit diese Verknüpfung selbst duchzuführen. Eine genauere Beschreibung findet sich in Goebel und Pauer (2014)[2]. Die Nutzung der inhaltlichen Indikatoren (ohne Verbindung zu den Geo-Koordinaten) erfolgt analog dem On-site-Zugriff der übrigen kleinräumigen Regionaldaten.

4.4. Remote Zugang von kontrollierten externen Zugangspunkten (SOEPremote-access)

In Kooperation mit externen Forschungseinrichtungen können Zugangspunkte für einen remote access zur Nutzung der unter 4.3.1 beschriebenen kleinräumigen Daten etabliert werden. Voraussetzung für die Etablierung eines solches Zugangspunktes ist der Abschluss eines Kooperationsvertrages, in dem unter anderem sichergestellt wird, dass die Administration des extern aufgestellten Thin Clients nur vom DIW Berlin aus möglich ist. Außerdem muss der externe Kooperationspartner zusichern, die am DIW Berlin implementierten technisch organisatorischen Maßnahmen des Gastarbeitsplatzes einzuhalten und zu kontrollieren.

4.5. Re-Analyse publizierter Ergebnisse

In zunehmendem Maße machen Zeitschriften die Veröffentlichung eines eingereichten Aufsatzes davon abhängig, dass die verwendeten Daten öffentlich zugängig gemacht werden. Dies verbietet aber der SOEP-Datenweitergabevertrag. Daher bietet das FDZ SOEP in diesen Fällen eine Archivierung von Analysedatensätzen an.

2 Goebel, Jan & Pauer, B. (2014). Datenschutzkonzept zur Nutzung von SOEPgeo im Forschungsdatenzentrum SOEP am DIW Berlin. Zeitschrift für amtliche Statistik Berlin-Brandenburg. 3. 42-47.

Welche Zugriffsbeschränkungen gelten, hängt von der Art der archivierten Daten ab, d. h. vom Grad der Anreicherung mit sensiblen Informationen; z. Bsp. von der Art der benutzten Geo-Informationen (siehe Tabelle 1). Die eingereichten Datensätze werden von den Mitarbeiterinnen bzw. Mitarbeitern des SOEP inhaltlich geprüft.

Anhang

Anhang A.1 Richtlinien für Gastaufenthalte

am Forschungsdatenzentrum (FDZ) des Sozio-oekonomischen Panels (SOEP) am DIW Berlin[1]

Der Zugang zu den faktisch anonymisierten SOEP-Daten im FDZ des SOEP erfolgt ausschließlich unter Einhaltung der geltenden Datenschutzregeln. Das FDZ ist zur Durchsetzung dieser Regeln und zur Überprüfung der Tätigkeit von Forscherinnen und Forschern, die Zugang zu den faktisch anonymen Forschungsdaten im Rahmen von Gastaufenthalten im FDZ erhalten, verpflichtet.

Die Mitarbeiter/innen des FDZ sind verpflichtet, ihren Einblick in Forschungsfragen, Methoden und Analysen der Gastwissenschaftler/innen nur zum Zwecke der Beratung, der Verbesserung des Service des FDZ sowie zur Gewährleistung der Einhaltung des Datenschutzes zu nutzen. Mitarbeiter/innen der. Abt. SOEP des DIW Berlin, die nicht unmittelbar für das FDZ arbeiten, erhalten keinen Einblick in die Tätigkeiten der Gastwissenschaftler/innen. Kooperationsprojekte zwischen Mitarbeiter/innen des SOEP und des FDZ einerseits und Gastforscher/innen andererseits sind hiervon nicht betroffen.

Der Aufenthalt von Gastwissenschaftlern im FDZ des SOEP ist an die Einhaltung folgender Regeln gebunden:

1. Den im allgemeinen Datennutzungsvertrag und den in der Vereinbarung über den Zugang zu faktisch anonymen Daten des SOEP im Rahmen von Gastaufenthalten im FDZ des SOEP getroffenen spezifischen Vereinbarungen zum Datenschutz, insbesondere dem Verbot des Versuchs der De-Anonymisierung, ist Folge zu leisten.

2. Gastforscher/innen erhalten Zugang zu speziellen datenschutzrechtlich geprüften Thin-Clients für die Zeit ihres Gastaufenthalts im FDZ und für die Durchführung des beantragten Projekts.

[1] Stand: Mai 2020

3. Gastwissenschaftler/innen erhalten einen Zugangscode (individuelle Kennung und Passwort) für den ihnen zugeteilten Thin-Client-Arbeitsplatz. Sie sind verpflichtet, diesen Code geheim zu halten und ihre Arbeitsstation gegen unbefugte Zugriffe oder Einsichtnahme Dritter in die Daten zu sperren, wenn sie den Raum verlassen.

4. Gastforscher/innen erhalten keinen Zugang zu PC-Arbeitsplätzen der SOEP-Mitarbeiter/-innen oder zu anderen als den in 2. benannten Thin-Client-Arbeitsplätzen.

5. Die Verwendung von mitgebrachten Laptops und Massenspeichern für die regional tiefer gegliederten SOEP-Daten ist untersagt.

6. Den Mitarbeiter/innen des FDZ ist es *im Prinzip* jederzeit erlaubt, Einblick in die Tätigkeiten der Gastforscher/innen zu nehmen, einschließlich deren Arbeitsmaterialien.

7. Gastforscher/innen erkennen an, dass alle Analyseergebnisse und sonstige Dateien, die sie aus den Räumen des SOEP-FDZ mitnehmen möchten, vorab von FDZ-Mitarbeiter/-innen datenschutzrechtlich geprüft und nachgesandt werden. Insbesondere unternehmen Gastforscher/innen keinen Versuch, Daten oder Datenauszüge aus den Räumen des SOEP-FDZ eigenständig mitzunehmen. Zur Ermöglichung der datenschutzrechtlichen Prüfung verpflichten Gastforscher/innen sich, alle durchgeführten Datenaufbereitungs- und Analyseschritte nachvollziehbar mit Hilfe von Programmsyntax durchzuführen und sich nach den Vorgaben in der Anleitung für Export von Ergebnissen zu richten.

8. Die Manipulation der technischen Ausstattung der Thin-Client-Arbeitsplätze ist Gastforscher/ innen strikt untersagt. Dies gilt einschließlich des Versuchs der Installation und der Ausführung von nicht durch das FDZ genehmigten Programmen.

9. Gastforscher/innen verpflichten sich, hinsichtlich Datenschutz und Datensicherheit das FDZ auf Sicherheitslücken hinzuweisen.

10. Gastforscher/innen verpflichten sich, das FDZ auf Mängel der Datenqualität hinzuweisen.

11. Verstöße von Gastwissenschaftler/innen gegen diese Bestimmungen führen zum sofortigen Abbruch des Gastaufenthalts und zur außerordentlichen Kündigung des dem Aufenthalt zugrunde liegenden Nutzungsvertrags und ggf. weiteren rechtlichen Konsequenzen.

Anhang A.2 Richtlinien für die Verwendung der SOEP-Daten in der Lehre[1]

Grundsätzlich können SOEP-Daten auch in der Lehre benutzt werden, aus datenschutzrechtlichen Gründen dürfen jedoch nur maximal 50 Prozent der Fälle ausgewählt werden. Es sei denn die Studenten werden mit einer Vertragsergänzung zu dem Datenweitergabevertrag mit hinzugefügt. Die Auswahl der 50 Prozent ist sehr einfach über die 'Random-Group-Variable' zu erreichen, die den Datenbestand in 20 Teilstichproben einteilt. Die Variable RGROUP20, die im Datensatz CIRDEF zu finden ist, hat 20 Ausprägungen. Für die Lehre dürfen nur die Fälle mit der Ausprägung 11 bis 20 benutzt werden.

Die Lehrversion kann vom SOEP als Download angefordert werden oder selbst erstellt werden. Fertige Skripte sind für SPSS, Stata und SAS vorhanden, mit deren Hilfe kann aus den installierten Originaldaten die Lehrversion erstellt werden.

Aus datenschutzrechtlichen Gründen dürfen Studenten in der Lehre auf keinen Fall Zugriff zu den Daten der Random-Groups 1-10 erhalten. Der Zugriff auf den Original-Datenbestand des SOEP verbietet sich daher von selbst. Es sei denn die Studenten werden mit einer Vertragsergänzung zu dem Datenweitergabevertrag mit hinzugefügt.

Der von unserer Vertragspartnerin/unserem Vertragspartner den Studenten bereitgestellte 'Lehr-Datensatz' muss auf einem gesonderten Plattenbereich liegen, dessen Zugang durch die Vertragspartnerin/dem Vertragspartner kontrolliert werden muss. Studentinnen/Studenten dürfen selbstverständlich keine Daten mit nach Hause nehmen oder 'irgendwo' innerhalb der Universität installieren.

Aus datenschutzrechtlicher Sicht ist die Vertragspartnerin/der Vertragspartner für die strikte Einhaltung des Datenschutzes verantwortlich! Deshalb sollten alle Studenten ebenso wie Ihre Mitarbeiter datenschutzrechtlich verpflichtet werden (das dazu erforderliche Formular ist auf der nächsten Seite).

Anhang B Datenschutzverpflichtungserklärungen

Anhang B.1 Verpflichtungserklärung für externe Nutzer

Verpflichtung

zur Beachtung des Datenschutzes

Hiermit erkläre ich, _____

dass ich bei meiner Arbeit mit den Datensätzen des DIW Berlin verpflichtet bin, die gesetzlichen Datenschutzvorschriften einzuhalten.

Nach diesen Regeln müssen personenbezogene Daten so verarbeitet werden, dass die Rechte der betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten nicht beeinträchtigt werden.

Nach den gesetzlichen Bestimmungen ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zu unbefugter Offenlegung oder zu unbefugtem Zugang mit den Daten führt. Außerdem müssen personenbezogene Daten vertraulich behandelt werden und dürfen nicht unbefugt an Dritte weitergegeben werden. Unterlagen mit personenbezogenen Daten sind so zu verwahren, dass sie vor dem Zugriff Dritter geschützt sind.

Mir ist außerdem bekannt, dass mir die Durchführung jeglicher Maßnahmen verboten ist, die zu einer Reidentifizierung der Befragungspersonen führen. Dasselbe gilt für die Publikation individueller Daten und die Zusammenführung der Daten mit anderen nicht anonymisierten SOEP-Daten. Auch dies ist streng verboten.

Mir ist bekannt, dass Verstöße gegen die Datenschutzvorschriften mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden können und dass das DIW Berlin bei Verstößen berechtigt ist, den Datennutzungsvertrag zu kündigen. Außerdem können dadurch Schadensersatzansprüche der betroffenen Personen begründet werden.

(Ort, Datum, Unterschrift)

Anlage zur Verpflichtung auf die Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO (Europäische Datenschutzgrundverordnung): „Personenbezogene Daten" [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „Verarbeitung" [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz").

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG (Bundesdatenschutzgesetz)

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Stand: Mai 2020

Anhang B.2 Begleitschreiben des Datenschutzbeauftragten des DIW Berlin (extern)

An alle SOEP-Datennutzer

Einhaltung des Datenschutzes beim Umgang mit SOEP-Daten

Sehr geehrte Damen und Herren,

die SOEP-Daten, die Ihre Institution auf der Grundlage eines Datenweitergabevertrages erhalten werden, sind hoch sensible Daten, die von allen Datennutzern, auch von Datennutzern im Ausland streng nach den gesetzlichen Bestimmungen, insbesondere der europäischen Datenschutzgrundverordnung (DSGVO) und nach unseren Datenschutzleitlinien zu behandeln sind.

Als betrieblicher Datenschutzbeauftragter des DIW Berlin bitte ich Sie deshalb um Beachtung folgender Hinweise bei der Nutzung der Daten des SOEP.

1. Bitte stellen Sie durch geeignete technische und organisatorische Maßnahmen sicher, dass die Daten vor unbefugtem Zugang geschützt sind. Dazu ist mindestens erforderlich:

- Verhinderung des Zugangs zu den Datenverarbeitungsanlagen und -systemen durch Unbefugte.
- Schutz des Zugriffs auf die Daten (inklusive aller Sicherheitskopien) durch Einrichtung von Passwörtern für Benutzerkennungen sowie regelmäßige Aktualisierung der Passwörter.
- Keine Datenfernverarbeitungen über das Internet.
- Keine Datenweitergabe an Unbefugte.
- Verpflichtung der zur Nutzung befugten Personen auf den Datenschutz.

2. Die Verbindung der SOEP-Daten mit Regionaldaten (Gemeindegrößenklassen, Raumordnungsregionen im Rahmen der SOEP Geo-codes) ist nur auf Grundlage eines erweiterten Datenweitergabevertrages und bei Etablierung weiterer Maßnahmen zum Schutz der Daten und deren Befolgung möglich.

3. Neben den beschriebenen Schutzmaßnahmen ist jeglicher Versuch einer Deanonymisierung der Daten streng untersagt und ein Verstoß gegen den mit dem DIW geschlossenen Datenweitergabevertrag, der zum Ausschluss von der Nutzung der SOEP-Daten führen kann. Bitte teilen Sie dies allen autorisierten Nutzerinnen und Nutzern mit.

4. Die SOEP-Daten werden für konkrete Forschungsvorhaben übermittelt. Falls Sie die Daten für ein neues Forschungsvorhaben nutzen wollen, müssen Sie dies dem SOEP rechtzeitig vor Beginn der Arbeiten, mitteilen. Dies gilt auch dann, wenn Sie Zweifel haben, ob ein neues Projekt noch unter den bestehenden Weitergabevertrag fällt.

5. Die SOEP-Daten erhalten Sie ausschließlich für die eigene wissenschaftliche Forschung, nicht für (entgeltliche oder unentgeltliche) Gutachten.

6. Die Nutzung der Daten ist auf die in Ihrem Antrag benannten **Beschäftigten** ihrer Institution bzw. auf die an Ihrer Institution **Promovierenden und Studierenden** beschränkt. Anderen Personen dürfen die SOEP-Daten nicht zugänglich gemacht werden, auch nicht in modifizierter Form.

7. Bei **Beendigung Ihrer Forschungsarbeiten,** sind die Ihnen übermittelten SOEP-Daten und evtl. Sicherungskopien, Auszugsdateien und Hilfsdateien vertragsgemäß zu löschen. Dies gilt auch für Daten die Promovierende und Studierende genutzt haben. Die Verantwortung auch für die Löschung der von diesem Personenkreis genutzten Daten liegt bei Ihrer Institution. Bitte instruieren und kontrollieren Sie die betreffenden Nutzer deshalb entsprechend.

8. Die Übertragung der Nutzungsbefugnis endet mit dem **Ausscheiden der nutzungsberechtigten Personen** aus der Institution, mit der wir den Datenweitergabevertrag geschlossen haben. Die Nutzung der SOEP-Daten an einer anderen Institution ist an den Abschluss eines **neuen** Datenweitergabevertrages mit dieser neuen Institution gebunden. Zusätzliche Voraussetzung ist eine schriftliche Bestätigung der bisherigen Institution darüber, dass die Daten gelöscht sind oder von einem anderen, durch einen Weitergabevertrag autorisierten SOEP-Nutzer genutzt werden. Bitte teilen Sie uns daher auch das Ausscheiden von autorisierten Datennutzern aus Ihrer Institution **unaufgefordert** mit.

8. Die Nutzung der SOEP-Daten für die **Lehre** ist nur unter folgenden Voraussetzungen möglich:

Es dürfen nicht mehr als 50% der Fälle des Standarddatensatzes genutzt werden (maximal die Random-Groups 11-20). Außerdem ist sicherzustellen, dass nach Abschluss von Lehrveranstaltungen keine SOEP-Daten bei den Studierenden verbleiben. Zudem müssen Sie die Nutzung dem SOEP anzeigen, bevor Sie die Daten in der Lehre einsetzen wollen.

Ich bitte Sie nachdrücklich um die Beachtung dieser Hinweise. Die strikte Einhaltung datenschutzrechtlicher Bestimmungen ist nicht nur vom Gesetz vorgeschrieben, sondern liegt im allgemeinen Interesse von Wissenschaft und Forschung.

Sprechen Sie mich gerne an, wenn Sie noch Fragen haben.

Mit freundlichen Grüßen

Thorsten Ritter
Datenschutzbeauftragter

agentia wirtschaftsdienst compliance
u. wenzel & t. ritter gbr
budapester straße 31
10787 berlin

SOEP
The German Socio-Economic
Panel Study at DIW Berlin

DIW Berlin – Deutsches Institut
für Wirtschaftsforschung e.V.
Mohrenstraße 58, 10117 Berlin
www.diw.de