



# SOEP | Datenschutzverfahren

Joachim R. Frick, Jan Goebel, Hansjörg Haas,  
Peter Krause, Ingo Sieber, Michaela Engelmann

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

Berlin, Februar 2010



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

### Inhaltsverzeichnis

1	Überblick.....	7
2	Lieferung der SOEP-Rohdaten von TNS Infratest an die Abteilung SOEP im DIW Berlin .....	11
3	Aufbereitung und Nutzung der SOEP Daten in der Abteilung SOEP des DIW Berlin .....	11
3.1	Aufbereitung der SOEP-Rohdaten in der Abteilung SOEP im DIW Berlin.....	11
3.2	Nutzung der SOEP-SUF- und Regionaldaten in der Abteilung SOEP und im DIW Berlin .....	12
3.2.1	SOEP-SUF-Daten.....	12
3.2.2	Regionaldaten.....	14
4	Zugang zu SOEP-Daten für DIW-Externe .....	15
4.1	Erst-Analysen .....	15
4.2	Re-Analyse publizierter Ergebnisse.....	16
	 Anhang	



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

Die Datenschutz-Grundphilosophie der Längsschnittstudie SOEP lautet seit Beginn der Studie im Jahr 1984: obwohl vom Erhebungsinstitut TNS-Infratest Sozialforschung (München) nur ausschließlich faktisch anonymisierte Mikrodaten nach Berlin geliefert werden, ist aus Sicherheitsgründen die Abteilung SOEP datenschutztechnisch vom Rest des DIW Berlin abgeschottet. Bei der Verarbeitung und der Weitergabe der faktisch anonymisierten Mikrodaten des SOEP gelten auf Basis einer Selbstverpflichtung des DIW Berlin hohe Sicherheitsstandards, die insbesondere bei der Nutzung von geo-referenzierten Informationen denen sehr nahe kommen, die für personenbezogene Daten gelten.

In Erinnerung sei gerufen: Nach § 3 Abs. 6 BDSG (BundesDatenSchutzGesetz; siehe [Anlage A.1](#)) bedeutet „Anonymisierung“ das Verändern personenbezogener Daten in derartiger Weise, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können. Faktisch orientiert sich die Längsschnittstudie SOEP an dem Konzept des BStG (BundesStatistikGesetzes) zur Übermittlung faktisch anonymisierter Daten. Teilweise werden die Daten wie personenbezogene Daten behandelt. Die Möglichkeit der Deklaration von deutlich „vergrößerten“ Daten als „absolut anonymisierte“ Daten (wie sie den Campus-Files der Amtlichen Statistik zugrunde liegt<sup>1</sup>) nutzt das SOEP bislang nicht.

Das DIW Berlin trägt die volle datenschutzrechtliche Verantwortung für die Datenerhebung zusammen mit dem Erhebungsinstitut TNS-Infratest Sozialforschung (München). Bei einem Wechsel des Erhebungsinstituts kann das DIW Berlin die Adressen der SOEP-Befragten erhalten und einem neuen Erhebungsinstitut zur Verfügung stellen. Das DIW Berlin ist zwar Eigentümer der Adressen, verzichtet jedoch im Zuge einer Selbstverpflichtung sowohl auf Kenntnis derselben sowie auf ein Speichern am Standort des DIW Berlin. Wenn Befragte im

---

<sup>1</sup> Vgl. z. B. <http://www.forschungsdatenzentrum.de/campus-file.asp> und [http://www.forschungsdatenzentrum.de/publikationen/fdz-allgemein/fdz\\_faltblatt\\_campus.pdf](http://www.forschungsdatenzentrum.de/publikationen/fdz-allgemein/fdz_faltblatt_campus.pdf).

DIW Berlin – in der Abteilung SOEP – anrufen, besteht somit keinerlei Möglichkeit diesen Anruf auf einen Datensatz zu beziehen. Wenn erforderlich, so wird in solchen Fällen auf Wunsch des Befragten ein Kontakt zu TNS-Infratest Sozialforschung (München) hergestellt.

# 1 Überblick

Obwohl vom Erhebungsinstitut TNS-Infratest Sozialforschung (München) nach Berlin ausschließlich faktisch anonymisierte Mikrodaten geliefert werden (vgl. Abschnitt 2 unten), ist aus Sicherheitsgründen die Abteilung SOEP datenschutztechnisch vom Rest des DIW Berlin völlig abgeschottet. Andere Abteilungen des DIW Berlin werden wie externe Datennutzer behandelt.

Innerhalb der Abt. SOEP gibt es folgende Kategorien von Zugriffsberechtigten:

- einen kleinen Kreis von Mitarbeitern, die Zugang zu allen von Infratest geliefert (Roh-) Daten haben (insb. Vornamen, Klartextangaben im Fragebogen, Postleitzahlen),
- einen noch kleineren Kreis (im Moment 2 Mitarbeiter), die auf einem Rechner, der isoliert innerhalb der Stabsabteilung Informationstechnik (IT) steht, Zugang zu Adressen-Koordinaten auf Hausblock-Ebene der Befragten hat<sup>1</sup>, und
- den Kreis der Mitarbeiterinnen und Mitarbeiter (einschließlich studentischer Mitarbeiterinnen und Mitarbeiter) und Gäste, die auf die stark anonymisierten SOEP-Scientific Use File-Daten (SUF des SOEP) und darüber hinaus auf Regionalkennungen (Gemeindegrößenklassen (GGK), BIK-Regionen sowie Raumordnungsregionen (ROR) bis hinab zu Kreiskennziffern Zugriff haben.<sup>2</sup>

Unter speziellen Sicherheitsstandards können Mitarbeiterinnen und Mitarbeiter (einschließlich studentischer Mitarbeiterinnen und Mitarbeiter) und Gäste Zugriff auf Informationen bis hinab zur Postleitzahl haben.

Externe Nutzerinnen und Nutzer erhalten nach Abschluss eines Datennutzungsvertrages standardmäßig die stark anonymisierten SUF-Daten. Nach Abschluss eines erweiterten Datennutzungsvertrages und Vorlage eines vom Datenschutzbeauftragten des DIW Berlin

---

<sup>1</sup> Diese Daten entsprechen der höchsten Sicherheitsstufe 3 in den Richtlinien zum Datenschutz des DIW Berlin.

<sup>2</sup> Im Prinzip entsprechen diese Daten der mittleren Sicherheitsstufe 2 in den Richtlinien zum Datenschutz des DIW Berlin. Im Rahmen einer freiwilligen Selbstverpflichtung ist der Zugang zu Daten auf Ebene von Kreiskennziffern stärker reglementiert.

geprüften Datenschutzkonzepts können externe Nutzerinnen und Nutzer der SOEP-Daten über das SUF hinaus die Gemeindegrößenklassen (GGK) und BIK-Regionen sowie Raumordnungsregionen (ROR) an ihrem Arbeitsplatz nutzen.

Es ist sicherlich erwähnenswert, dass trotz des großen Kreises von Mitarbeiterinnen und Mitarbeitern, von studentischen Hilfskräften und Gästen, die im Laufe von über 25 Jahren mit den besonders sensiblen Daten des SOEP gearbeitet haben, niemals auch nur einen Verdacht auf Deanonymisierung eines Befragten gab.

Es gehört nicht nur zur Datenschutzverpflichtung, sondern zum Berufsethos der Mitarbeiterinnen und Mitarbeiter, dass sie auch Befragte, die sich ihnen gegenüber zu erkennen geben (was z. B. der Projektleiter innerhalb von fast 20 Jahren zweimal erlebt hat), keinesfalls im Datensatz zu finden versuchen.

Für das SOEP gibt es bislang kein frei downloadbares CAMPUSfile (siehe dazu z. B. <http://www.forschungsdatenzentrum.de/campus-file.asp>), das als absolut anonymisiert angesehen wird. Auch die Lehrversion des SOEP wird nicht als absolut anonymisiert, sondern nur als faktisch anonymisiertes Datenfile betrachtet.<sup>1</sup> Zu den dazugehörigen Verpflichtungen der Lehrenden und Studierenden siehe [Anhang A.3](#).

Für ein Lehrbuch<sup>2</sup> wurden kleinere Datensätze erzeugt, die absolut anonymisiert sind, da alle SOEP-üblichen IDs (Personen- und Haushaltsnummern) vollständig entfernt, die Fallzahl und die Zahl der Variablen drastisch reduziert und alle objektiven Variablen mit einem Zufallsfehler belegt wurden.<sup>3</sup>

---

1 Die Lehrversion des SOEP umfasst zurzeit 50 % der Fälle und keinerlei über das Bundesland hinausgehende Regionalinformationen.

2 Siehe Kohler, Ulrich und Frauke Kreuter (2008): Datenanalyse mit Stata. Allgemeine Konzepte der Datenanalyse und ihre praktische Anwendung, 3. Auflage, Oldenbourg Verlag: München und Wien.

3 Der erste von Kohler und Kreuter (2008) genutzte Datensatz 1 (Erhebungsjahr 1997) umfasst 3340 Fälle und 47 Variablen. Das entspricht 25 % der Zahl der Beobachtungen in der originären SOEP-Datei und 8 % der maximal möglichen Variablen. Der zweite im Lehrbuch verwendete Datensatz (Längsschnitt 1984-1997) besteht aus 1288 Fällen und 115 Variablen. Dies entspricht 5 % der maximal möglichen Fälle und knapp 20 % der möglichen Variablen.

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 Wissenschaftler in der Abt. SOEP	Externe Wissenschaftler mit DNV
SOEP Namen und Adressen	-/-	-/-	-/-	-/-
SOEP-Rohdaten	AV + DSV + eingeschränkter Benutzerkreis	-/-	-/-	-/-
SOEP-Standard (SUF)	AV + DSV	AV + DSV	DNV + DSV	DNV + lokale DSV
Gemeindegrößenklassen und BIK-Regionen	AV + DSV	AV + DSV	DNV + DSV	DNV + ZV 1 + DSK
Raumordnungsregionen	AV + DSV	AV + DSV	DNV + DSV	DNV + ZV 2 + DSK
Kreise	AV + DSV	AV + DSV	DNV + DVS + SOEPonsite oder DNV + DVS + SOEPremote	DNV + ZV 3
Postleitzahlen	AV + DSV	AV + DSV + SOEPonsite mit protokolliertem Zugriff	DNV + DVS + SOEPonsite mit protokolliertem Zugriff	-/-
Microm Zusatzdaten	AV + DSV	AV + DSV	DNV + DVS + SOEPonsite auf unvernetztem Rechner ohne externe Speichermedien	-/-
Klartextangaben	AV + DSV + Nutzung auf Anfrage	-/-	Nutzung auf Anfrage auf unvernetztem Rechner ohne externe Speichermedien	-/-
In Erprobungsphase: Geo-Koordinaten	AV + DSV + stark eingeschränkter Benutzerkreis + spezielle Serverumgebung innerhalb der IT des DIW Berlin	-/-	-/-	-/-
Archiv für Re-Analysen	AV + DSV + ggf. eingeschränkter Benutzerkreis	AV + DSV + ggf. weitere Maßnahmen <sup>1)</sup>	AV + DV + ggf. weitere Maßnahmen <sup>1)</sup>	DNV + lokale DSV + ggf. ZV <sup>1)</sup>

AV: Arbeitsvertrag; DSV = Datenschutzverpflichtung; DNV = Datennutzungsvertrag; ZV = Zusatzvertrag; DSK = vom DIW Berlin geprüftes Datenschutzkonzept, SOEPonsite = Nutzung in den Räumen der Abt. SOEP mit zusätzlicher Verpflichtung; -/- = Kein Zugriff erlaubt

<sup>1)</sup> Welche Einschränkungen greifen, hängt von der Art der archivierten Daten ab.

## **2 Lieferung der SOEP-Rohdaten von TNS Infratest an die Abteilung SOEP im DIW Berlin**

Die Erhebungsdaten des Sozio-oekonomischen Panels (SOEP) werden vom Erhebungsinstitut – TNS-Infratest Sozialforschung in München – zur weiteren Bearbeitung und Aufbereitung am DIW Berlin an den zuständigen verantwortlichen Mitarbeiter persönlich adressiert und Passwort geschützt als Wertbrief zugestellt.

Die Adressangaben und Namen der Befragten werden noch im Erhebungsinstitut sofort von den Befragungsdaten getrennt und verbleiben beim Erhebungsinstitut.

Das DIW Berlin erhält ausschließlich faktisch anonymisierte Mikrodaten. Alle personenbeziehbaren Angaben aus den laufenden Erhebungen werden durch die Verwendung von verschlüsselten Personen- und Haushalts-IDs anonymisiert ausgeliefert.

## **3 Aufbereitung und Nutzung der SOEP Daten in der Abteilung SOEP des DIW Berlin**

### **3.1 Aufbereitung der SOEP-Rohdaten in der Abteilung SOEP im DIW Berlin**

Die mit der Aufbereitung der Original-Erhebungsdaten des SOEP betrauten Mitarbeiter/-innen unterliegen gesonderten datenschutzrechtlichen Maßnahmen; sie sind neben der Einhaltung der Datenschutzbestimmung bei der Verarbeitung personengebundener Daten auch auf die Sicherung des Datenzugangs verpflichtet. Das bedeutet, dass jeder Computer, auf dem Daten des SOEP gespeichert sind, nur mit einer personalisierten Nutzerkennung und Passwort-Kombination benutzbar ist und dass bei Nicht-Benutzung (Idle) über mehrere nutzen automatisch eine neue Identifizierung erfragt wird.

Die vom Erhebungsinstitut eingehenden Daten (SOEP-Rohdaten) werden in der Abteilung SOEP im DIW Berlin auf einem gesondert gesicherten Server unter einer eigenen Kennung

gespeichert, zu der nur die direkt verantwortlichen Mitarbeiter/-innen Zugang haben (dies sind in der Regel drei Mitarbeiter/-innen, die beim Datenschutzbeauftragten als Bearbeiter/-innen gelistet sind; nur sie haben die nötigen Passwörter). Ausschließlich diesen Mitarbeitern ist es vorbehalten, die Daten jahresübergreifend in einer Datenbank zusammenzuführen.

Bei der Aufbereitung dieser SOEP-Rohdaten für die standardmäßige wissenschaftliche Weiternutzung werden als weitere Datenschutzmaßnahmen Klartextangaben<sup>1</sup> sowie alle über das Bundesland hinausgehenden regional differenzierenden Merkmale gelöscht. Dieser weniger sensitive Datensatz, die so genannten SOEP-SUF-Daten, ist Basis für die weitere nutzerfreundliche Aufbereitung der SOEP-Daten, die anschließend per DVD im Rahmen der Datenweitergabe an lizenzierte und datenschutzrechtlich verpflichtete Nutzerinnen und Nutzer gehen (siehe [Abschnitt 4](#)).<sup>2</sup>

## **3.2 Nutzung der SOEP-SUF- und Regionaldaten in der Abteilung SOEP und im DIW Berlin**

### **3.2.1 SOEP-SUF-Daten**

Nach der Prüfung und Aufbereitung sowie der Durchführung der datenschutz-relevanten Maßnahmen werden die SOEP-SUF-Daten für die standardmäßige wissenschaftliche Nutzung vom Datenmanagement der Abteilung SOEP bereitgestellt. Dazu werden die für die wissenschaftliche Nutzung verfügbaren Daten aus der SIR-Datenbank in drei Analyseformate (SPSS, SAS, STATA) ausgelesen und auf einem gesondert gesicherten Server für die Datenweitergabe und inhaltliche Analyse bereitgestellt. Auf den Server mit den faktisch hochanonymisierten und zur Weitergabe freigegebenen SOEP-SUF-Daten können Mitarbeiter/-innen erst zugreifen nach Einrichten einer persönlichen Nutzerkennung mit individuellem Passwort und der Verpflichtung zur Einhaltung datenschutzrechtlicher Nutzungsbestimmungen.

---

<sup>1</sup> Klartextangaben umfassen Berufs- und Bildungsbezeichnungen und weitere offene Angaben der Interviewten sowie Vornamen (Vornamen dienen der Kontrolle der korrekten Verknüpfung verschiedener personenbezogener Teildatensätze in den von TNS Infratest gelieferten SOEP-Rohdaten).

<sup>2</sup> Der Datenumfang der Datenweitergabe ist noch zusätzlich beschränkt, er beinhaltet z.B. keine direkten Daten aus dem Lebenslauffragebogen.

Dies gilt auch für Gäste des SOEP, denen dann nach Unterzeichnung der Datenschutzerklärung eine Gastkennung für den Datenzugang eingerichtet wird. Dieselben Maßnahmen gelten auch für Mitarbeiter/-innen des DIW Berlin aus anderen Abteilungen. Jeder Gastwissenschaftler ist einer/einem SOEP Mitarbeiter/-in (Betreuer/-in) zugeordnet, diese/dieser Mitarbeiter/-in füllt den Antrag auf eine Nutzerkennung aus und bestätigt mit ihrer/seiner Unterschrift die Notwendigkeit der verschiedenen Datenzugänge. Administriert werden die Nutzerkennung zentral von der Stabsabteilung Informationstechnik (IT) wie auch alle normalen Mitarbeiter/innenkennungen. Alle Gäste werden ebenso wie Mitarbeiterinnen und Mitarbeiter des DIW Berlin datenschutzrechtlich verpflichtet (siehe [Anhang B.1.a](#)) und genießen somit quasi „Mitarbeiter/-innenstatus“; sowohl bei den Rechten wie bei den Pflichten.

Die anonymisierten Mikrodaten des SOEP werden anderen Abteilungen des DIW Berlin mit Hilfe der Standard-Datenweitergabe-DVDs Passwort geschützt zur Verfügung gestellt. Andere Abteilungen – ausgenommen der Abteilung SOEP – können nicht auf die intern gespeicherten Rohdaten des SOEP zugreifen.

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

Alle weitergehenden Nutzungen des SOEP – wie etwa die Nutzung von Klartextangaben, tiefer gegliederten Regionalmerkmale oder auch die Verknüpfung mit anderen Datensätzen durch spezifische, datenschutzrechtlich anerkannte Verfahren des „Statistical Matching“ können nur nach Absprache mit den Verantwortlichen der Abteilung SOEP erfolgen und unterliegen jeweils weitergehenden personenbezogenen Datenschutzverpflichtungen und ggf. zusätzlichen technisch-organisatorischen Maßnahmen. Die direkte Verknüpfung personenbezogener Daten aus dem SOEP mit entsprechenden Einträgen identischer Personen aus anderen Datenbeständen oder Registern („Record Linkage“) ist rechtlich ausgeschlos-

sen und aufgrund fehlender eindeutiger Schlüssel (Name, Sozialversicherungsnummer, etc.) weder technisch noch praktisch möglich.

### 3.2.2 Regionaldaten

Die Nutzung der Regionalinformationen auf der Ebene der ca. 400 Landkreise (inkl. kreisfreier Städte) ist ausschließlich am DIW Berlin möglich, die damit zugänglichen Daten liegen auf jeweils nur für diese Person zugänglichen Bereichen. Diese Informationen dürfen aus datenschutzrechtlichen Gründen nicht außerhalb des DIW Berlin analysiert werden.

Damit auch jenen externen Wissenschaftlerinnen und Wissenschaftlern, denen es nicht möglich ist, direkt vor Ort am DIW Berlin zu sein, die Nutzung der Kreisdaten ermöglicht wird, gibt es zudem einen kontrollierten Datenfernverarbeitungszugang (SOEPremote): Nach Unterzeichnung und Prüfung eines speziellen Vertrages können Wissenschaftler/-innen ihre Auswertungssyntax an eine bestimmte E-Mail-Adresse am DIW Berlin senden und bekommen die auf Einhaltung des Datenschutzes kontrollierten Ergebnisse wieder zurück gesendet. Bei diesem international bewährten Verfahren (das sich bei der Luxembourg Income Study seit Jahren bewährt hat und von dort gekauft wurde) hat zu keiner Zeit die/der Wissenschaftler/-in außerhalb des DIW Berlin direkten Zugriff auf die Mikrodaten und diese werden zu keinem Zeitpunkt außerhalb des DIW Berlins verarbeitet.

Für die Nutzung der Postleitzahlen der Befragungshaushalte in Verbindung mit den Daten des SOEP steht für Gäste im DIW Berlin eine besondere Schnittstelle zur Verfügung. Ähnlich dem Remote-Zugriff haben die Nutzer keinen direkten Zugriff auf die Daten und jegliche ausgeführte Auswertungssyntax wird personalisiert protokolliert. Client und Server dieses Zugangs sind beide nur innerhalb des DIW Intranet verfügbar. Intern ist der Zugang zu Postleitzahlen-Daten standardmäßig nur jenen SOEP-Mitarbeitern möglich, die auch Zugriff auf die Rohdaten haben.

Für methodische Experimente innerhalb der Abteilung SOEP zur Zuspierung von Häuserblock genauen Regionaldaten und Fernbeobachtungsdaten (Satellitendaten) wurde eine spezielle (bislang nur experimentelle) Serverumgebung innerhalb der IT des DIW Berlin aufgebaut („SOEPgeo“), die sicherstellt, dass kein Nutzer dieser hochsensiblen Daten zugleich Zugang zu diesen kleinräumigen Regionaldaten und den SOEP-Daten besitzt. D.h., selbst die/der analysierende Wissenschaftler/-in kann nicht auf den Verknüpfungsalgorithmus zugreifen.

Dieser Datenzugang besteht bisher in der experimentellen Testphase nur für drei ausgewählte Personen im SOEP und wird auf seine Datensicherheit und Nutzbarkeit.

## **4 Zugang zu SOEP-Daten für DIW-Externe**

### **4.1 Erst-Analysen**

Die Nutzung der anonymisierten SOEP-Daten außerhalb des DIW Berlin erfolgt nur für wissenschaftliche Zwecke auf der Grundlage eines Weitergabevertrages an die antragstellende Universität oder außeruniversitäre Forschungseinrichtung. Private Unternehmen und Personen sind von der Nutzung ausgeschlossen; für Drittmittelforschung kann in Ausnahmefällen ein Datenweitergabevertrag abgeschlossen werden. Hierfür werden detaillierte Projektbeschreibungen eingefordert.

Der Vertrag enthält neben der institutionellen Anbindung auch eine zeitliche Befristung, die Angabe des Forschungszwecks sowie die Verpflichtung zur Einhaltung datenschutzrechtlicher Maßnahmen vor Ort. Der Nutzungsvertrag wird mit der Datennutzerin/dem Datennutzer persönlich abgeschlossen. Damit soll die unmittelbare persönliche Verantwortung eines Datennutzers sichergestellt werden.

Erst nach Abschluss dieses Vertrages werden die für die wissenschaftliche Nutzung des SOEP freigegebenen Daten auf DVD Passwort geschützt ausgeliefert. Nutzer im außereuropäischen Ausland (streng genommen: außerhalb der EU und der EU datenschutzrechtlich gleichgestellten Länder Schweiz, Norwegen und Liechtenstein) haben zudem nur Zugang zu einer 95%-Zufallsstichprobe der ersten Welle des kompletten SOEP-Datenbestandes.<sup>1</sup>

Die Nutzung von Gemeindegrößenklassen, BIK-Regionen oder Regionalinformationen auf der Ebene der 97 Raumordnungsregionen außerhalb des DIW Berlin ist nur nach Vorlage eines erweiterten Datenschutzkonzeptes und der Prüfung dessen durch den Datenschutzbeauftragten des DIW Berlin möglich.

Externe Nutzer, die mit tiefergegliederten Regionalinformationen arbeiten wollen, müssen SOEPremote nutzen (zurzeit nur für Kreiskennziffern möglich) oder als Gäste ins DIW Berlin kommen.

## 4.2 Re-Analyse publizierter Ergebnisse

In zunehmendem Maße machen Zeitschriften die Veröffentlichung eines eingereichten Aufsatzes davon abhängig, dass die verwendeten Daten öffentlich zugänglich gemacht werden.<sup>2</sup>

Da die Weitergabe des SOEP-Datensatzes durch die Nutzer grundsätzlich nicht erlaubt ist, bieten wir allen Nutzern die Möglichkeit, entsprechende Datensätze im SOEP-FDZ-Archiv für Re-Analysen zu speichern.

Welche Zugriffsbeschränkungen gelten, hängt von der Art der archivierten Daten ab, d. h. vom Grad der Anreicherung mit sensiblen Informationen; d. h. in den meisten Fällen: von der Art der benutzten Geo-Informationen (siehe [Tabelle 1](#)).

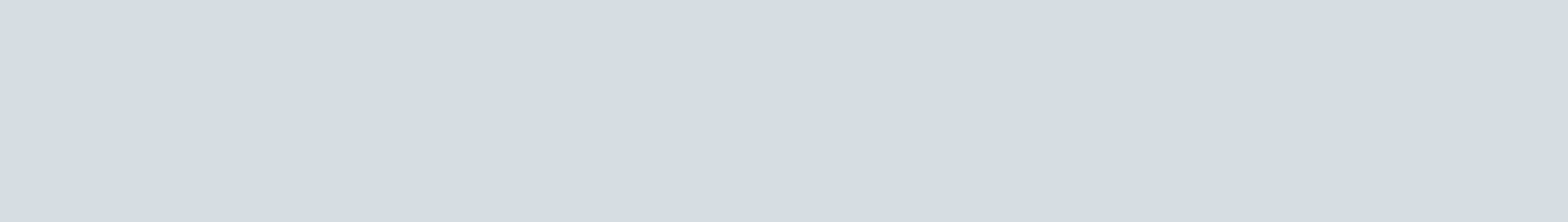
Die eingereichten Datensätze werden von den Mitarbeitern des SOEP inhaltlich geprüft und dann dem Datenschutzbeauftragten zur Unterschrift vorgelegt.

---

<sup>1</sup> Durch das Löschen von 5 % der Fälle wird der Versuch der Deanoymisierung einen Befragten deutlich erschwert, da ein Angreifer nicht weiß, ob ein Datensatz, der einer realen Person ähnlich sieht, von dieser Person stammt oder von einer der nicht-zugänglichen 5 %.

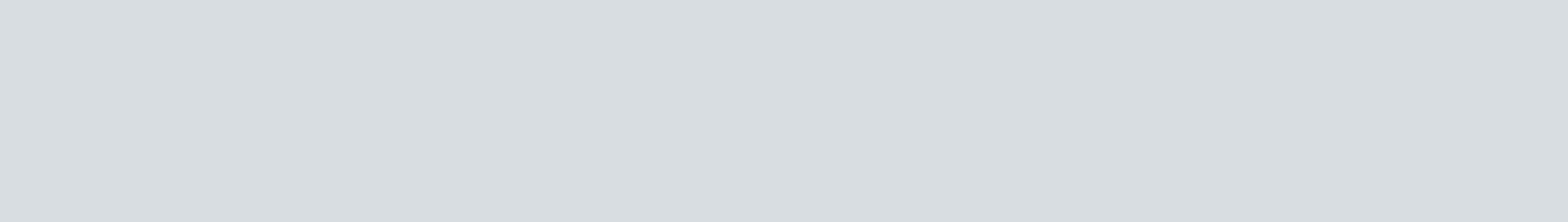
<sup>2</sup> Siehe z. B. Klepper et al, 2009, p. 96-57.

Wir bieten freilich auch in diesem Falle eine Archivierung im FDZ SOEP als Service an. Absolute Anonymisierung kann oft erreicht werden, indem die Zahl der Variablen und Beobachtungen auf das minimal notwendige Maß reduziert und die SOEP-Personen- und Haushaltsnummern durch beispielsweise fortlaufende Nummern ersetzt werden. Eine solchermaßen „absolut anonymisierte“ Datei ist dem SOEP zur Prüfung und Freigabe vorzulegen.



# Anhang

Anhang A	Gesetzliche Grundlagen und Richtlinien .....	21
Anhang A.1	Auszüge aus dem Bundesdatenschutzgesetz (BDSG) .....	21
Anhang A.2	Richtlinien für Gastaufenthalte.....	28
Anhang A.3	Richtlinien für die Verwendung der SOEP-Daten in der Lehre.....	31
Anhang B	Datenschutzverpflichtungserklärungen .....	33
Anhang B.1.a	Verpflichtungserklärung für externe Nutzer .....	33
Anhang B.1.b	Begleitschreiben des Datenschutzbeauftragten des DIW Berlin (extern)..	34



## Anhang A Gesetzliche Grundlagen und Richtlinien

### Anhang A.1 Auszüge aus dem Bundesdatenschutzgesetz (BDSG)

Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (BGBl. I, S. 2814) Aktualisierte, nicht amtliche Fassung.

#### **Herausgeber:**

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Stand:

01. September 2009

#### **Anmerkung:**

Die Änderungen durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254) und Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] sind noch nicht in dieser Fassung enthalten, weil sie erst zum 01. April 2010 bzw. 11. Juni 2010 in Kraft treten. Im Hinblick auf die in § 47 enthaltene Übergangsregelung ist die bisher geltende Fassung des § 28 weiterhin in Kursivschrift wiedergegeben.

### § 3 Weitere Begriffsbestimmungen

- (1) **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
- (2) **Automatisierte Verarbeitung** ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.
- (3) **Erheben** ist das Beschaffen von Daten über den Betroffenen.
- (4) **Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
  1. **Speichern** das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
  2. **Verändern** das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
  3. **Übermitteln** das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
    1. die Daten an den Dritten weitergegeben werden oder
    2. der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten ein- sieht oder abruft,
  4. **Sperren** das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
  5. **Löschen** das Unkenntlichmachen gespeicherter personenbezogener Daten.

- (5) **Nutzen** ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.
- (6) **Anonymisieren** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
- (6a) **Pseudonymisieren** ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
- (7) **Verantwortliche Stelle** ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
- (8) **Empfänger** ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
- (9) **Besondere Arten personenbezogener Daten** sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
- (10) **Mobile personenbezogene Speicher- und Verarbeitungsmedien** sind Datenträger,
1. die an den Betroffenen ausgegeben werden,
  2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(11) Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

## **§ 5 Datengeheimnis**

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

## **§ 43 Bußgeldvorschriften**

- (1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,
- 2.a entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,
- 2.b entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,
3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,
- 5.a entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,
6. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,
7. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
8. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
9. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,
10. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
11. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

12. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
13. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abrufmittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abrufen oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,
- 5.a entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,
- 5.b entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,
6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

- (3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

## Anhang A.2 Richtlinien für Gastaufenthalte

### **am Forschungsdatenzentrum (FDZ) des Sozio-oekonomischen Panels (SOEP) am DIW Berlin<sup>1</sup>**

Der Zugang zu den faktisch anonymisierten SOEP-Daten im FDZ des SOEP erfolgt ausschließlich unter Einhaltung der geltenden Datenschutzregeln (insbesondere §5 und §40, Abs.1 BDSG). Das FDZ ist zur Durchsetzung dieser Regeln und zur Überprüfung der Tätigkeit von Forscherinnen und Forschern, die Zugang zu den anonymisierten Sozialdaten 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 anonymisierten 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 PC-Arbeitsplätzen für die Zeit ihres Gastaufenthalts im FDZ und für die Durchführung des beantragten Projekts.

---

<sup>1</sup> Stand: Juli 2009

3. Gastwissenschaftler/innen erhalten einen Zugangscode (individuelle Kennung und Passwort) für den ihnen zugeteilten PC-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 PC-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 gegebenenfalls 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.
8. Die Manipulation der technischen Ausstattung der PC-Arbeitsplätze ist Gastforscher/innen strikt untersagt. Dies gilt einschließlich 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.3 Richtlinien für die Verwendung der SOEP-Daten in der Lehre<sup>1</sup>

Grundsätzlich können SOEP-Daten auch in der Lehre benutzt werden, aus datenschutzrechtlichen Gründen dürfen jedoch nur maximal 50 Prozent der Fälle ausgewählt werden. Diese Auswahl 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 selbst erstellt werden: In der Dokumentation der DVD befindet sich unter dem Punkt 'Data add ons' der Link zu einem entsprechenden Programm, das eine 50%-Lehrversion erstellt. 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.

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

---

<sup>1</sup> Stand: Januar 2009.

sowie ein Begleitschreiben des Datenschutzbeauftragten des DIW Berlin, Herrn Alexander Eickelpasch, kann unter:

<http://www.diw.de/documents/dokumentenarchiv/17/43535/dsform.366501.pdf>

abgerufen werden (s. hierzu auch Anhang B.1 auf der nächsten Seite).

## Anhang B Datenschutzverpflichtungserklärungen

### Anhang B.1.a Verpflichtungserklärung für externe Nutzer

Stand: 18.06.99

#### Verpflichtung zur Wahrung des Datengeheimnisses

Frau/Herr \_\_\_\_\_

Abteilung/Projekt \_\_\_\_\_

wird hiermit auf die Wahrung des Datengeheimnisses nach § 5 Bundesdatenschutzgesetz (BDSG) verpflichtet. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit.

Hierzu weisen wir auf folgendes hin:

Nach § 5 BDSG ist es den bei der Datenverarbeitung beschäftigten Personen **untersagt, Daten unbefugt zu verarbeiten oder zu nutzen**, d.h. diese Daten dürfen Sie nur zur rechtmäßigen Erfüllung der Ihnen übertragenen Aufgaben speichern, verändern, übermitteln, sperren, löschen oder auf sonstige Weise nutzen. Jede unbefugte Verarbeitung oder Nutzung für andere Zwecke ist untersagt.

Die Weitergabe personenbezogener Daten an Dritte ist nur in Sonderfällen, für die eine ausdrückliche Erlaubnis vorliegen muß, zulässig. Unterlagen mit personenbezogenen Daten und personen-bezogenen Dateien sind so zu verwahren, daß sie vor dem Zugriff Dritter geschützt sind. Zum Schutz der Daten ist im Rahmen der übertragenen Aufgabe die notwendige Sorgfalt anzuwenden; festgestellte Mängel sind dem Datenschutzbeauftragten zu melden.

Verstöße gegen das Datengeheimnis können nach § 43 BDSG und anderen einschlägigen Rechtsvorschriften mit Geld- oder Freiheitsstrafen geahndet werden. Eine Verletzung des Datengeheimnisses stellt in den meisten Fällen gleichzeitig ein Verstoß gegen arbeitsvertragliche Pflichten dar und kann arbeitsrechtliche Maßnahmen zur Folge haben.

Fragen zum Datenschutz beantwortet Ihnen gerne Ihr(e) Datenschutzbeauftragte(r).

Bitte bestätigen Sie durch Ihre Unterschrift, daß Sie diese Erläuterung gelesen und Ihre Verpflichtung auf das Datengeheimnis zur Kenntnis genommen haben.

\_\_\_\_\_  
Datum/Unterschrift des /der Verpflichteten

Original:            Datenschutzbeauftragte(r)

1. Kopie:            Mitarbeiterin/Mitarbeiter

2. Kopie:            Personalakte

## **Anhang B.1.b Begleitschreiben des Datenschutzbeauftragten des DIW Berlin (extern)<sup>1</sup>**

An alle SOEP-Datennutzer

### **Erfordernisse des Datenschutzes beim Umgang mit den SOEP-Daten**

Sehr geehrte Damen und Herren,

die SOEP-Daten, die Sie auf der Grundlage eines Datenweitergabevertrages erhalten werden, sind sensitive Daten. Die Bestimmungen des Bundesdatenschutzgesetzes sind von allen einzuhalten, auch von den Datennutzern im Ausland. Deshalb wende ich mich an Sie mit der Bitte um Beachtung folgender Hinweise:

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

- Verschlussene Aufbewahrung der Originaldatenträger und der evtl. Sicherungskopien,
- Verschlussene Aufbewahrung der datensatzbeschreibenden Materialien, getrennt von den Datenträgern),
- Verhinderung des Zugangs zu den Datenverarbeitungsanlagen und –systemen durch Unbefugte,
- Schutz des Zugriffs auf die Daten durch Einrichtung von Passwörtern für Benutzerkennungen sowie regelmäßige Aktualisierung der Passwörter,
- Keine Datenfernverarbeitung,
- Keine Datenweitergabe an Unbefugte,
- Verpflichtung der befugten Personen auf den Datenschutz (ein Muster einer Verpflichtungserklärung liegt bei).

Falls weitergehende Maßnahmen zum Schutz der Daten möglich sind, sollten Sie diese ergreifen. Die oder der Datenschutzbeauftragte Ihrer Institution wird Sie sicherlich gerne beraten.

Die SOEP-Daten werden Ihnen für ein oder mehrere konkrete Forschungsvorhaben übermittelt. Falls Sie die Daten für ein neues Forschungsvorhaben nutzen wollen, ist dies in der Regel möglich, indem Sie dies der SOEP-Gruppe rechtzeitig, also vor Beginn der Arbeiten, mitteilen. Wenn Sie Zweifel haben, ob ein neues Projekt noch in den Rahmen des bestehenden Vertrages passt, fragen Sie bitte vorsichtshalber bei der SOEP-Gruppe im DIW Berlin an. Bitte beachten Sie, dass Sie die SOEP-Daten nur für die eigene wissenschaftliche Forschung, nicht

---

<sup>1</sup> Stand: 02.2006

für (entgeltliche oder unentgeltliche) Gutachten erhalten haben. Wenn Sie Gutachten erstellen wollen, ist eine Vertragsergänzung notwendig, über die Sie mit dem SOEP-Projektleiter, Herrn Professor Dr. Gert Wagner, sprechen sollten.

Durch den Datenweitergabevertrag ist die Datennutzung inhaltlich auf das angegebene Forschungsvorhaben und personell auf Sie und die in Ihrem Forschungsprojekt beteiligten **Mitarbeiterinnen und Mitarbeiter** beschränkt. Sie dürfen die SOEP-Daten nicht an andere Personen oder Institutionen weitergeben oder sie ihnen zugänglich machen, auch nicht in modifizierter Form. Wenn **Doktoranden und Diplomanden**, die mit den SOEP-Daten arbeiten sollen, nicht in einem Arbeitsverhältnis zu Ihnen stehen, teilen Sie uns dies bitte rechtzeitig unter namentlicher Nennung des/der Doktoranden/Diplomanden mit; bitte teilen Sie uns auch den (Arbeits-)Titel und die voraussichtliche Dauer der Promotion/Diplomarbeit mit. Nach Abschluss der Arbeit sind Sie dafür verantwortlich, dass der Doktorand/Diplomand seine Datensätze löscht. Ihre studentischen oder wissenschaftlichen Hilfskräfte, die in einem Arbeitsverhältnis zu Ihnen stehen, müssen nicht gemeldet werden.

Bei **Beendigung Ihrer Forschungsarbeiten**, für die Sie die SOEP-Daten angefordert haben, sind die übermittelten Daten und evtl. Sicherungskopien, Auszugsdateien und Hilfsdateien vertragsgemäß zu löschen. Sollte diese Situation bei Ihnen eintreten, teilen Sie uns das bitte mit; der Vertrag zwischen Ihnen und dem DIW läuft damit aus.

Die Übertragung der Nutzungsrechte an Sie endet auch mit Ihrem **Ausscheiden** aus der datenempfangenden Institution. Wenn Sie beispielsweise an eine andere Universität wechseln und dort weiterhin mit SOEP-Daten arbeiten wollen, ist ein neuer Datenweitergabevertrag erforderlich. Voraussetzung dafür ist Ihre schriftliche Bestätigung, dass Sie die Daten an Ihrer alten Institution gelöscht oder einem anderen autorisierten SOEP-Nutzer (mit einem eigenen Datenweitergabevertrag) übergeben haben. Der Verbleib der SOEP-Daten muss auch dann geklärt werden, wenn Sie zukünftig nicht mehr mit den Daten arbeiten wollen. Bitte teilen Sie uns Ihr Ausscheiden aus Ihrer bisherigen Institution **unaufgefordert** mit.

Bei Beachtung der folgenden beiden Bedingungen ist eine Nutzung von Teilen des SOEP-Standarddatensatzes in der **Lehre** grundsätzlich möglich: Es darf sich nur um höchstens 50% der Fälle des Standarddatensatzes handeln (maximal die Random-Groups 11-20). Außerdem ist sicherzustellen, dass nach Abschluss jeder Lehrveranstaltung keine SOEP-Daten bei den Studierenden verbleiben. Dies würde eine unzulässige Datenweitergabe darstellen und hätte den Entzug des Nutzungsrechts durch das DIW Berlin zur Folge. Wenn Sie die Daten in der Lehre einsetzen wollen, sollten Sie dies der SOEP-Gruppe anzeigen.

Ich bitte nachdrücklich um Beachtung dieser Hinweise. Die strikte Einhaltung datenschutzrechtlicher Bestimmungen ist nicht nur vom Gesetz vorgeschrieben, sondern auch im allgemeinen Interesse der Forschung. Eine Wiederholungsbefragung wie das SOEP ist ganz besonders auf die Einhaltung der datenschutzrechtlichen Erfordernisse angewiesen. Für Rückfragen stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen



Alexander Eickelpasch