Datenschutz Merkblatt

BASE II
Berliner Altersstudie II

Allen BASE-II Datennutzern
zur Kenntnisnahme

Charité –
Universitätsmedizin Berlin
Humboldt-Universität zu Berlin
Max-Planck-Institut für
Bildungsforschung, Berlin
Sozio-oekonomisches Panel
Universität zu Lübeck
Universität Tübingen

Erfordernisse des Datenschutzes beim Umgang mit den BASE-II-Daten
Anlage zum Datenweitergabevertrag

Berlin, den 5. Juni 2018

Kontakt:
BASE-II
c/o Max-Planck-Institut für Bildungsforschung
Dr. Ludmila Müller
Lentzeallee 94
D-14195 Berlin
lmueller@mpib-berlin.mpg.de
0049.30.82406-380

Sehr geehrte Damen und Herren,

die BASE-II-Daten, die Sie auf der Grundlage eines Datenweitergabevertrags erhalten werden, sind sensitive Daten. Die Bestimmungen der Europäischen Datenschutzgrundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) 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:

- Verschlossene Aufbewahrung der Originaldatenträger und der evtl. Sicherungskopien,
- Verhinderung des Zugangs zu den Datenverarbeitungsanlagen durch Unbefugte,
- Schutz des Zugriffs auf die Daten durch Passwörter und deren regelmäßige Aktualisierung,
- keine Datenfernverarbeitung,
- keine Datenweitergabe an Unbefugte,
- Verpflichtung der befugten Personen auf den Datenschutz (Muster einer Verpflichtungserklärung liegt bei).

Ihre Datenhaltung der gelieferten BASE-II-Daten dokumentieren Sie bitte in einem Datenschutzkonzept, das von dem/der Datenschutzbeauftragen Ihrer Einrichtung unterschrieben werden muss. Enthalten sein müssen die folgenden Angaben:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

Schutz vor physischem Zutritt: Wie wird sichergestellt, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird? Beschreibung des Ortes/Rechnertyps, auf dem die Daten gespeichert werden sollen.

Zugangskontrolle: Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können? U.a.: Prozedur zur Verhinderung der Nutzung der Daten auf anderen Rechnern (auch nicht auf dem heimischen PC); Verfahren zum regelmäßigen Wechsel von Passwörtern

Zugriffskontrolle: Wie wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können? Auch: Wer wird mit den Daten arbeiten?

Trennungskontrolle: Wie stellt der Auftragnehmer sicher, dass Daten des Auftraggebers von sonstigen Datenbeständen getrennt werden?

2. Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

Weitergabekontrolle: Wie wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?

Eingabekontrolle: Wie wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?

3. Betriebskontinuität und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

Betriebskontinuitätsmanagement: Wie wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind?

4. Auftragskontrolle (Art. 28 Abs. 3 lit. a), lit b), 32 Abs. 4 DS-GVO)

Auftragskontrolle: Der Auftragnehmer stellt sicher, dass allen von ihm eingesetzten Beschäftigten vor Aufnahme ihrer Tätigkeit alle für sie relevanten Datenschutzvorgaben bekannt sind. Hierzu gehören insbesondere die Anweisungen des Auftraggebers zur Erbringung der [im Leistungsverzeichnis / in der Verdingungsunterlage / im Vertrag] festgelegten Leistungen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DS-GVO, Art. 25 Abs. 1 DS-GVO)

Beschreibung der internen/externen Audits und Managementbewertung

Im Falle der Nutzung hochsensibler Daten können weitere Sicherheitsmaßnahmen erforderlich sein. Bitte wenden Sie sich an die BASE-II Koordination (Dr. Katrin Schaar, schaar@mpib-berlin.mpg.de)

Die BASE-II-Daten werden Ihnen für Forschungsvorhaben überlassen. Falls Sie die Daten für ein neues Forschungsvorhaben nutzen wollen, ist dies in der Regel möglich, indem Sie dies der BASE-II-Koordination 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 BASE-II-Koordination an. Bitte beachten Sie, dass Sie die BASE-II-Daten nur für die eigene wissenschaftliche Forschung, nicht für (entgeltliche oder unentgeltliche) Gutachten nutzen dürfen.

Durch den Datenweitergabevertrag ist die Datennutzung inhaltlich auf das angegebene Forschungsvorhaben und personell auf Sie und die in Ihrem Antrag als Datennutzer genannten Personen beschränkt.

Sie sind dafür verantwortlich, dass weitere Datennutzer bei BASE-II gemeldet werden und dass diese die Daten nur nutzen dürfen, sofern Sie den Konditionen der Datennutzung entsprechend Ihres Vertrags zugestimmt haben sowie eine Datenschutzerklärung bei BASE-II abgegeben haben.
Nach Abschluss der Arbeiten sind Sie dafür verantwortlich, dass die weiteren Datennutzer ihre/seine Datensätze löscht/löschen.

Datenschutz Merkblatt

Bei Beendigung Ihrer Forschungsarbeiten, für die Sie die BASE-II-Daten verwendet haben, sind die übermittelten Daten, evtl. Sicherungskopien, Auszugsdateien und Hilfsdateien vertragsgemäß zu löschen. Im Fall, dass die Daten auf Grund von Anforderungen wissenschaftlicher Verlage oder Zuwendungsgeber für eine längere Periode nach der Publikation vorgehalten werden müssen (z.B. für 7 oder 10 Jahre), müssen die Daten nach Beendigung dieses Zeitraums gelöscht werden. Bitte benachrichtigen Sie die/den BASE-II-Koordinator/in.

Die Übertragung der Nutzungsrechte an Sie endet auch dann, wenn Sie aus der Einrichtung ausscheiden, der Sie derzeit angehören. Wenn Sie beispielsweise an eine andere Universität wechseln und dort weiterhin mit BASE-II-Daten arbeiten wollen, müssen Sie dies BASE-II über die/den Koordinator/in mitteilen. Voraussetzung dafür ist Ihre schriftliche Bestätigung, dass die Daten an Ihrer alten Institution gelöscht werden. Bitte teilen Sie der BASE-II-Koordination Ihr Ausscheiden aus Ihrer bisherigen Institution unaufgefordert mit.

Wir bitten nachdrücklich um die Beachtung dieser Hinweise. Die strikte Einhaltung datenschutzrechtlicher Bestimmungen ist nicht nur vom Gesetz vorgeschrieben, sondern auch im allgemeinen Interesse der Forschung. Eine Wiederholungsbefragung wie BASE-II ist ganz besonders auf die Einhaltung der datenschutzrechtlichen Erfordernisse angewiesen.

Mit freundlichen Grüßen

Für das BASE-II Leitungsgremium

Prof. Dr. Denis Gerstorf

Der BASE-II Vertragstext nutzt bei der Antragsgestaltung weitgehend die Standards und Vorlagen des DIW/SOEP. BASE-II bedankt sich für die freundliche Überlassung der Vorlagen.