Vereinbarung über die Überlassung von Daten zum Zwecke der Durchführung von Monitoring und Evaluation der ESF-Fördermaßnahmen des Landes Baden-Württemberg in der ESF-Förderperiode 2014-2020

zwischen dem

Land Baden-Württemberg, Ministerium für Soziales und Integration, nachfolgend bezeichnet als SM, vertreten durch Gerald Engasser

und

der ISG Institut für Sozialforschung und Gesellschaftspolitik GmbH, Weinsbergstraße 190, 50825 Köln, nachfolgend bezeichnet als ISG, vertreten durch Herrn Dr. Dietrich Engels.

Präambel

Die Vertragsparteien haben eine Leistungsvereinbarung geschlossen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Landesdatenschutzgesetzes (LDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1
Vertragsgegenstand

(1) Gegenstand dieser Vereinbarung sind Regelungen im Zusammenhang mit der Übermittlung von Daten über ESF-geförderte natürliche und juristische Personen zur Durchführung von Monitoring und Evaluation der ESF-Fördermaßnahmen des Landes Baden-Württemberg.
(2) Inhalt und Umfang der Nutzungsberechtigung der übermittelten Daten sowie die datenschutzrechtlichen Sicherheitsmaßnahmen, die beim Umgang mit den personen- und unternehmensbezogenen Daten einzuhalten sind, richten sich nach dieser Vereinbarung. Im Übrigen gelten die einschlägigen datenschutzrechtlichen Bestimmungen, insbesondere die Europäische Datenschutz-Grundverordnung (DSGVO) und das Landesdatenschutzgesetz Baden-Württemberg.
(3) Das Evaluationsvorhaben beruht auf dem Angebot der ISG zur Durchführung der ESF-Evaluation in Baden-Württemberg vom 14.03.2014, dem ab 07.07.2014 wirksamen Vertrag zwischen dem SM und der ISG über die Durchführung der Evaluation sowie dem von der ISG vorgelegten Bewertungsplan.

§ 2
Datenbereitstellung

(1) ISG erhält vom SM die Berechtigung, personen- und unternehmensbezogene Daten über Teilnehmende (einschließlich Existenzgründer/innen) und Unternehmen an ESF-Fördermaßnahmen zu erheben, zu speichern und weiter zu verarbeiten.
(2) Die Berechtigung umfasst zum einen pseudonymisierte Datensätze mit Merkmalen der geförderten natürlichen Personen gemäß Anhang I der Verordnung (EU) Nr. 1304/2014. Diese Daten werden durch die L-Bank erhoben und gespeichert und über eine gesicherte, technische Einrichtung durch SM an ISG geliefert. Darüber hinaus werden Kontaktinformationen der natürlichen Personen zum Zwecke der Evaluation sowie zu den in der Verordnung (EU) Nr. 1304/2014 genannten Zwecken (Erhebung der längerfristigen Ergebnisindikatoren) durch ISG von den Zuwendungsempfängern in einem dafür geeigneten, gesicherten Verfahren abgerufen.
(3) Für juristische Personen einschließlich Selbstständige und Einzelunternehmer werden ISG nicht-pseudonymisierte Informationen über eine gesicherte, technische Einrichtung zur Verfügung gestellt.

§ 3
Datenschutz

(1) ISG ist verpflichtet, die datenschutzrechtlichen Bestimmungen einzuhalten.
(2) Die übermittelten personen- und unternehmensbezogenen Daten dürfen nur für den in § 1 genannten Zweck genutzt werden. Eine Verwendung zu einem anderen Zweck ist nicht zulässig. Eine Weitergabe an Dritte ist nur an Unterauftragnehmer gemäß § 4 erlaubt. Nicht zulässig ist die Weitergabe an sonstige Drille oder die gewerbliche Nutzung (insbesondere im Rahmen von Gutachten für private Auftraggeber).
(3) ISG stellt sicher, dass die Daten nur denjenigen Mitarbeiter/inne/n der ISG zugänglich gemacht werden, die mit der Bearbeitung des in § 1 bezeichneten Forschungsvorhabens betraut sind. Diese Personen sind gemäß § 78 SGB X zu unterrichten und zu verpflichten.
(4) Die mit der Evaluation betrauten Personen sind namentlich zu dokumentieren. Die Aufnahme neuer Mitarbeiter/innen in das Evaluationsvorhaben ist fortlaufend zu dokumentieren. Die Dokumentation ist dem SM auf Verlangen vorzulegen.

(5) Alle diese Mitarbeiter/innen haben sich ISG gegenüber vor dem Zugänglichmachen der Daten schriftlich zu verpflichten, jede Handlung zu unterlassen:
- die darauf abzielt oder geeignet ist, die personenbezogenen Daten zu veröffentlichen oder an Drille im Sinne von § 3 (2) weiterzugeben.
- die darauf abzielt oder geeignet ist, die in der Datenbasis enthaltenen nicht anonymisierten Einzeldaten oder deren Aggregate zu veröffentlichen oder an Dritte weiterzugeben.

(6) Eine Zusammenführung der an ISG übermittelten oder durch Weiterverarbeitung entstandenen Individualdaten mit anderen Individualdaten ist nicht erlaubt. Erlaubt ist jedoch die Zusammenführung gemäß § 4 (1) und (2) dieser Vereinbarung.

§ 4
Unterauftragnehmer

(1) ISG ist berechtigt, zum Zwecke der Durchführung von telefonischen Befragungen einen Unterauftragnehmer einzuschalten. ISG darf in diesem Fall die Kontaktdaten der Teilnehmer/innen an den Unterauftragnehmer weiterleiten.
(2) ISG ist berechtigt, einen Unterauftragnehmer einzuschalten, der einen Abgleich der gemäß § 2 (2) dieser Vereinbarung erhobenen Daten mit den prozessproduzierten Daten der Bundesagentur für Arbeit durchführt. ISG ist berechtigt, solche Daten an den Unterauftragnehmer weiterzugeben, die ausschließlich der Identifikation der Teilnehmer/innen in den prozessproduzierten Daten der Bundesagentur für Arbeit dienen. Die aus dem Abgleich resultierenden zusätzlichen Daten darf ISG zu den in § 1 dieser Vereinbarung genannten Zwecken nutzen.
(3) Unterauftragnehmern sind die Pflichten nach § 6 dieses Vertrages aufzuerlegen.

§5
Anforderungen an Unterauftragnehmer

(1) In den Fällen gemäß § 4 (1) und (2) ist die Befragungs- bzw. Datenabgleichsabsicht und der Forschungszweck gegenüber den betroffenen Personen zu erläutern, auf die Freiwilligkeit der Teilnahme hinzuweisen sowie die Einwilligung der Betroffenen einzuholen und zu dokumentieren. Die Namen, Anschriften, E-Mailadressen und Telefonnummern der Personen sind von den Ergebnissen der Befragung bzw. des Abgleichs getrennt zu speichern. Eine Verbindung darf nur über eine Pseudo-ID herstellbar sein.
(2) Der Unterauftragnehmer übermittelt seine Daten (ohne Namen, Anschriften und Telefonnummern) verschlüsselt auf einem externen Datenträger an ISG. Bei telefonischen Befragungen werden alle teilnehmerbezogenen Daten vom entsprechenden Unterauftragnehmer in einem sicheren Verfahren unverzüglich nach Abschluss des Auftrags gelöscht.

§ 6
Datensicherheit

(1) ISG hat durch die im Anhang aufgeführten technischen und organisatorischen Maßnahmen sicherzustellen, dass nur die Personen, die am Forschungsprojekt arbeiten, Zugang zu der Datenbasis haben und auch alle anderen daten- schutzrechtlichen Anforderungen gewährleistet werden.
(2) Werden Änderungen der technischen und organisatorischen Maßnahmen vorgenommen, so sind diese von ISG schriftlich zu fixieren und vom SM genehmigen zu lassen.

§ 7
Geheimhaltung

(1) Veröffentlichungen unter Verwendung von personen- und unternehmensbezogenen Daten müssen den Vorschriften des Sozialdatenschutzes und den Geheimhaltungsvorschriften des Bundesstatistikgesetzes entsprechen, insbesondere dürfen Veröffentlichungen keine Rückschlüsse auf Personen oder Unternehmen ermöglichen.
(2) ISG haftet für alle Schäden, die SM aus dem nicht vereinbarungsgemäßen, unzulässigen oder unrichtigen Umgang mit den übermittelten Daten entstehen und stellt SM insoweit von Haftungsansprüchen Dritter frei.

§ 8
Löschungspflicht

(1) Alle übermittelten und durch Weiterverarbeitung entstandenen Daten sind so früh wie möglich, spätestens jedoch zum Ende der aus dem Evaluationsauftrag resultierenden Aufbewahrungspflichten durch ISG vollständig und sicher zu löschen.
(2) überlassene Datenträger sind unverzüglich zurückzugeben oder sicher zu löschen.
(3) Die ordnungsgemäße Löschung der Daten wird protokolliert und ist SM auf Verlangen schriftlich anzuzeigen.

§ 9
Kontrollrechte

(1) ISG erklärt sich damit einverstanden, dass SM Auskünfte bei ihr einholt, während der Geschäftszeiten nach Terminvereinbarung seine Geschäftsräume betritt und dort Besichtigungen und Prüfungen vornimmt und geschäftliche Unterlagen, gespeicherte Daten und Datenverarbeitungsprogramme einsieht, soweit dies erforderlich ist, um die Einhaltung der Vorschriften dieser Vereinbarung zu prüfen.
(2) Der Auftragnehmer unterwirft sich auch der Kontrolle durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, soweit Daten des Auftraggebers betroffen sind.

§ 10
Sonstige Bestimmungen

(1) Änderungen dieser Vereinbarung sind nur gültig, wenn sie in Schriftform erfolgen.
(2) Sollte eine Bestimmung dieser Vereinbarung ungültig sein, betrifft dies nicht die Vereinbarung als Ganzes. In einem solchen Fall ist die Vereinbarung ihrem Sinn und Zweck entsprechend auszulegen, wobei zu berücksichtigen ist, was die Parteien gewollt hätten, wenn ihnen die Ungültigkeit einer Bestimmung dieser Vereinbarung bekannt gewesen wäre.

Stuttgart, den 2.7.2018

Gerald Engasser
Ministerium für Soziales und Integration
Baden-Württemberg

Köln, den 2.7.2018

Dr. Dietrich Engels
ISG Institut für Sozialforschung
und Gesellschaftspolitik GmbH

Anhang „Technisch-organisatorische Maßnahmen"

zur Datenschutzvereinbarung vom 2.7.2018 zwischen dem Land Baden-Württemberg, Ministerium für Soziales und Integration (SM), und der ISG Institut für Sozialforschung und Gesellschaftspolitik GmbH (ISG).

§ 6 der Datenschutzvereinbarung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation

ISG wird die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	Die Mitarbeiter von ISG arbeiten in der Regel in den Büroräumlichkeiten des Instituts. Unbefugten wird der Zugang zu den mobilen und Desktop-Rechnern, mit denen personenbezogene und/oder Befragungsdaten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt: Die Räumlichkeiten des Instituts sind an beiden Standorten (Köln/Berlin) mit einer Sicherheitsschließanlage geschützt. Die Räumlichkeiten der einzelnen Mitarbeiter/innen werden zusätzlich während ihrer Abwesenheit von ihnen abgeschlossen.
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Zur Verhinderung der Nutzung des Datenverarbeitungssystems durch Unbefugte wird der Zugang zu mobilen und Desktop-Rechnern durch einen Passwortschutz mit regelmäßigem Passwortwechsel (mindestens monatlich) geschützt. Die regelmäßige Überprüfung der Sicherheitsmaßnahmen und der Wechsel der Passwörter obliegen dem Systemadministrator. Er weist die zugangsberechtigten Personen in die Schutzvorkehrungen ein und setzt sie über die erforderlichen Passwörter in Kenntnis. Hinsichtlich der Passwortstärke orientiert sich ISG an den Sicherheitsempfehlungen des BSI.
3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Zur Gewährleistung, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, wurde folgende Vorkehrung getroffen: Die Daten werden über einen Online-Speicher eines in der Schweiz ansässigen, zertifizierten (ISO 27001 und ISO/IEC 27001) Hosters ausgetauscht. Dieser wurde von ISG explizit im Rahmen der Sorgfaltspflichten des § 62 Bundesdatenschutzgesetz (BDSG) als Dienstleister ausgewählt. Die ausschließlich in europäischen Mitgliedsstaaten (Niederlande, Irland) befindlichen Server des Hosters verfügen über die Zertifizierungen ISO 27001, SSAE16 sowie weitere

		Zertifizierungen. Der Datenaustausch ist den befugten Mitarbeitern/innen nur über spezielle, passwortgeschützte Clients möglich, die lokal auf den Rechnern der Mitarbeiter/innen eingerichtet werden müssen. Vor dem Transport auf den bzw. die Server werden die Daten clientseitig Ende-zu-Ende verschlüsselt (AES-256, RSA-2096). Der Datentransport ist ebenso verschlüsselt. Ein Zugang zu Daten auf der Online-Cloud ist ausschließlich berechtigten Nutzern möglich. Nur die für die relevanten Forschungsvorhaben explizit genannten Mitarbeiter/innen haben Zugriff auf speziell für Sie eingerichtete Projektverzeichnisse auf dem Onlinespeicher.
4.	**Weitergabekontrolle** Es ist zu gewährleisten, 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.	Zur Gewährleistung, dass personenbezogene und andere Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, werden folgende Vorkehrungen getroffen: • Die mobilen Datenträger werden im Institut in Schränken verschlossen aufbewahrt. • Es wird zugesichert, dass erhaltene personenbezogene oder andere Daten an niemanden außerhalb des Projektteams weitergegeben werden. • Alle Mitarbeiter/innen des Projektteams erhalten Einweisungen zu datenschutzrechtlichen Grundlagen (insbesondere zu den Betroffenenrechten) und Einweisungen zu den Datensicherheitsvorkehrungen, an denen sie mitwirken müssen (insbesondere, dass es strengstens untersagt ist, Daten auf andere als die institutseigenen Datenträger zu übertragen).
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene und Befragungsdaten verändert oder entfernt worden sind, werden alle Übertragungsvorgänge von Daten auf der unter Punkt 3 beschriebenen Online-Cloud versioniert. Alle Bearbeitungsschritte autorisierter Nutzer von Projektverzeichnissen werden hierbei automatisch protokolliert. Die Erstellung, Bearbeitung und Löschung von Dateien auf mobilen und Desktop-Rechnern kann vom Systemadministrator durch entsprechende Logdaten reproduziert werden.
6.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Dateien mit personenbezogenen und sonstigen Daten werden auf der hochgradig verschlüsselten Online-Cloud im hierfür vorgesehenen Projektverzeichnis gespeichert und lokal, d.h. auf den mobilen oder Desktop-Rechnern befugter Projektmitarbeiter/innen synchronisiert. Alle Bearbeitungsschritte der Mitarbeiter/innen werden auf der Online-Cloud als Versionen einer Datei gespeichert. Versehentlich gelöschte Dateien können von berechtigten Projektmitarbeitern/innen wiederhergestellt werden. Alle (verschlüsselten) Dateien werden in verschiedenen Bereichen auf den Servern des von ISG beauftragten Hosters gespiegelt. Dies minimiert das Verlustrisiko von Daten. Die Rechenzentren des beauftragten Hosters werden zudem kontinuierlich bewacht, um unautorisierten Zugang und weitere Ausfälle zu verhindern.

7.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Die Daten werden, wie unter Punkt 2 (Zugangskontrolle) und 3 (Zugriffskontrolle) beschrieben, a) auf mobilen und Desktop-Rechnern befugter Mitarbeitern/innen sowie b) auf einer hochgradig verschlüsselten Online-Cloud gespeichert. Dieser Onlinespeicher ist nur über ein spezielles Rechte-Rollen-Konzept zugänglich. Zugriff hierauf haben ausschließlich autorisierte Projektmitarbeiter/innen. ISG verwendet grundsätzlich getrennte Projektverzeichnisse und den speziellen Zwecken entsprechende Unterverzeichnisse in den vorgenannten Dateisystemen.

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

Stuttgart, den 2.7.2018

Gerald Engasser
Ministerium für Soziales und Integration
Baden-Württemberg

Köln, den 2.7.2018

Dr. Dietrich Engels
ISG Institut für Sozialforschung
und Gesellschaftspolitik GmbH