Vereinbarung über die Überlassung von Daten zum Zwecke der Durchführung von Monitoring und Evaluation der ESF-Plus-Fördermaßnahmen des Landes Baden-Württemberg in der Förderperiode 2021-2027

zwischen dem
Land Baden-Württemberg, Ministerium für Soziales, Gesundheit und Integration, nachfolgend bezeichnet als SM, vertreten durch Herrn Dr. Matthias Boll

und

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

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-Plus-geförderte natürliche und juristische Personen zur Durchführung von Monitoring und Evaluation der ESF-Plus-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-Plus-Evaluation in Baden-Württemberg vom 17.01.2022 und dem ab 15.03.2022 wirksamen Vertrag zwischen dem SM und der ISG über die Durchführung der Evaluation.

§ 2
Datenbereitstellung

(1) ISG erhält vom SM die Berechtigung, Daten über Teilnehmer*innen und Projektträger aus ESF-Plus-Fördermaßnahmen zu erheben, zu speichern und weiter zu verarbeiten. Hierzu zählen auch Daten mit Personenbezug.
(2) Die Berechtigung umfasst zum einen pseudonymisierte Datensätze mit Merkmalen der geförderten natürlichen Personen gemäß Anhang I der Verordnung (EU) Nr. 2021/1057. Diese Daten werden durch die L-Bank erhoben und gespeichert und über eine gesicherte, technische Einrichtung durch das SM an ISG geliefert. Darüber hinaus werden Kontaktinformationen der natürlichen Personen zum Zwecke der Evaluation sowie zu den in der Verordnung (EU) Nr. 2021/1057 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*innen, 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 ggf. 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 Dritte oder die gewerbliche Nutzung (insbesondere im Rahmen von Gutachten für private Auftraggeber).
(3) ISG stellt sicher, dass die Daten nur denjenigen Mitarbeiter*innen 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 Dritte 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 sind jedoch die Zusammenführung gemäß § 4 (1) und (2) dieser Vereinbarung sowie die Ergänzung durch von ISG durchgeführte Befragungen.

§ 4
Unterauftragnehmer

(1) ISG ist berechtigt, zum Zwecke der Durchführung von telefonischen oder postalischen Befragungen einen Unterauftragnehmer einzuschalten. ISG darf in diesem Fall die Kontaktdaten der Teilnehmer*innen an den Unterauftragnehmer weiterleiten und durch diesen zusätzlich erhobene Individualdaten mit den durch das SM übermittelten Daten zusammenführen.
(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 § 5 dieser Vereinbarung aufzuerlegen.

§ 5
Anforderungen an Unterauftragnehmer

(1) In den Fällen gemäß § 4 (1) und (2) sind 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 – technisch gesichert – getrennt zu speichern. Eine Verbindung darf nur über eine Pseudo-ID herstellbar sein.
(2) Der Unterauftragnehmer übermittelt seine gemäß § 4 (1) und (2) ermittelten Daten (ohne Namen, Anschriften, E-Mailadressen und Telefonnummern) in digitaler Form über einen verschlüsselten Transportweg an ISG. Nach Durchführung der Befragungen werden alle teilnehmer*innenbezogenen 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 datenschutzrechtlichen 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 dem SM aus dem nicht vereinbarungsgemäßen, unzulässigen oder unrichtigen Umgang mit den übermittelten Daten entstehen und stellt das 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 dem SM auf Verlangen schriftlich anzuzeigen.

§ 9
Kontrollrechte

(1) ISG erklärt sich damit einverstanden, dass das 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/die Landesbeauftragte*n 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 31.05.2022

Dr. Matthias Boll
Ministerium für Soziales, Gesundheit und Integration
Baden-Württemberg

Köln, den 31.05.2022

Dr. Philipp Fuchs
ISG Institut für Sozialforschung
und Gesellschaftspolitik GmbH

Anhang „Technisch-organisatorische Maßnahmen“

zur Datenschutzvereinbarung vom 31.05.2022 zwischen dem Land Baden-Württemberg, Ministerium für Soziales, Gesundheit 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.
Alle Mitarbeiter*innen von ISG sind grundsätzlich dem Datenschutz verpflichtet und werden sowohl zu Beginn ihres Beschäftigungsverhältnisses als auch regelmäßig im Laufe ihrer Tätigkeiten datenschutzrechtlich unterwiesen. Zudem werden alle am Datenverarbeitungsprozess beteiligten Mitarbeiter*innen von ISG, die Zugang zu den zu verarbeitenden Daten erhalten, in die projektspezifischen Datenschutzbelange eingewiesen.

§ 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*innen 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 Schließanlage geschützt. Die Räumlichkeiten der einzelnen Mitarbeiter*innen werden zusätzlich während ihrer Abwesenheit von ihnen abgeschlossen. Eine Verarbeitung von personenbezogenen Daten in Privatwohnungen der Mitarbeiter*innen der ISG (Telearbeitsplätze, Heimarbeitsplätze) darf nur nach vorheriger Zustimmung erfolgen. Die Datenschutzkonformität der Telearbeitsplätze wird gewährleistet. Dazu sind von allen Mitarbeiter*innen die ISG-Mitarbeiter*inneninformationen "Datenschutz im Homeoffice" zu berücksichtigen. Die Telearbeitsplätze sind so gestaltet, dass unbefugte Dritte keine Kenntnis von personenbezogenen Daten nehmen können.
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 geschützt. Mobile und Desktop-Rechner sind vollverschlüsselt. Die regelmäßige Überprüfung der Sicherheitsmaßnahmen obliegt dem/der Systemadministrator*in der ISG. Sie/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. Alle Arbeitsrechner sind mit Anti-Virus-Software-Clients ausgestattet und so konfiguriert, dass ein hoher Sicherheitsstandard der Geräte gewährleistet werden kann. Die Internetverbindung in den Bürostandorten ist zusätzlich durch eine Firewall gesichert.
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 ein Open-Source Cloudsystem eines in Deutschland ansässigen, zertifizierten Hosters ausgetauscht. Dieser wurde von ISG explizit im Rahmen der Sorgfaltspflichten des § 62 Bundesdatenschutzgesetz (BDSG) als Dienstleister ausgewählt. Das gehostete System befindet sich in einem in Deutschland befindlichen Interxion-Rechenzentrum, das ISO-27001-zertifiziert ist sowie die Zertifizierungen für „Business Continuity Management Systems" BS 25999-2:2007 und für den „Payment Card Industry Data Security Standard" erfolgreich durchlaufen hat. Der Datenzugriff ist ausschließlich berechtigten ISG-Mitarbeiter*innen möglich. Nur die für die relevanten Forschungsvorhaben explizit genannten Mitarbeiter*innen haben Zugriff auf speziell für sie eingerichtete Projektverzeichnisse des Cloudsystems. Darüber hinaus, ist es auch Administrator*innen der IT-Abteilung der ISG technisch möglich, auf Projektverzeichnisse zuzugreifen. Eine Einsichtnahme in projektbezogene Daten ist diesen Nutzern aber qua gesonderter Datenschutzvereinbarung für die IT-Abteilung untersagt. Technisch geschützt wird der Zugriff auf das Cloudsystem über eine Zwei-Faktor-Authentifizierung. Sichere Passwörter werden über eine entsprechende Passwortrichtlinie systemseitig sichergestellt. Der Datentransport ist hochgradig verschlüsselt. Besonders sensible Daten können bei Bedarf im System Ende-zu-Ende verschlüsselt werden.
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: • (Verschlüsselte) mobile 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). • Der Datenaustausch von projektbezogenen Daten über das Cloudsystem erfolgt verschlüsselt.
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 des unter Punkt 3 beschriebenen Cloudsystems versioniert. Alle Bearbeitungsschritte autorisierter Nutzer von Projektverzeichnissen werden hierbei automatisch protokolliert. Die Erstellung, Bearbeitung und Löschung von Dateien auf mobilen und Desktop-Rechnern kann von Projektverantwortlichen und von Systemadministrator*innen 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 dem verschlüsselten Cloudsystem 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 dem Cloudsystem als Versionen einer Datei gespeichert. Versehentlich gelöschte Dateien können von berechtigten Projektmitarbeiter*innen wiederhergestellt werden. Alle (verschlüsselten) Dateien werden in verschiedenen Bereichen auf den in Deutschland befindlichen 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 Mitarbeiter*innen sowie b) auf einem verschlüsselten Cloudsystem gespeichert. Das Cloudsystem 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) Seitens der ISG wurde ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgesehenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert. Die nachfolgend genannten Maßnahmen sind hierbei von besonderer Relevanz:

Nr.	Maßnahme	Umsetzung der Maßnahme
8.	**Datenschutz-Management**	• Alle Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter*innen nach Bedarf / Berechtigung werden zentral dokumentiert. • Ein ISG-weit gültiges Datensicherheitskonzept liegt vor. • Es gibt eine/n interne/n Datenschutzbeauftragte*n (DSB) und eine/n

		interne/n Informationssicherheitsbeauftragte*n (ISB) mit entsprechenden Zuständigkeiten für die Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs. • ISG-weit erfolgt eine regelmäßige (mind. jährliche) Sensibilisierung der Mitarbeiter*innen zum Thema Datenschutz und -sicherheit. • Eine Datenschutz-Folgenabschätzung (DSFA) kann bei Bedarf durchgeführt werden. • Ein formalisierter Prozess zur Bearbeitung von Auskunftsfragen seitens Betroffener ist vorhanden. • Die ISG kommt den Informationspflichten nach Art. 13 und Art. 14 DSGVO nach.
9.	**Incident-Response-Management** Maßnahmen zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen	ISG-weit zum Einsatz kommen regelmäßig aktualisierte Netzwerküberwachungs-, Firewall-, Spamfilter- und Virenschutz-Software. Hierüber sind ein technisches Monitoring und technische Maßnahmen zur Behebung von Sicherheitsverletzungen möglich. DSB und ISB sind in das Incident-Response-Management eingebunden.
10.	**Datenschutzfreundliche Voreinstellungen** gem. § 24 Abs. 2 DSGVO	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Stuttgart, den 31.05.2022

Dr. Matthias Boll
Ministerium für Soziales, Gesundheit und Integration
Baden-Württemberg

Köln, den 31.05.2022

Dr. Philipp Fuchs
ISG Institut für Sozialforschung
und Gesellschaftspolitik GmbH