Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherung BSV
Direktionstab DS – IT Management ITM

eGov Mitteilung Nr. 056 vom 26.05.2025

Geht an: Durchführungsstellen der 1. Säule/FamZ

Betreff: Vorgaben zu Verträgen mit Dritten

Mit dem Trend zur Auslagerung von IT-Dienstleistungen und modernen Sourcing-Möglichkeiten beziehen die Durchführungsstellen der 1. Säule/FamZ vermehrt IT-Dienstleistungen von Dritten.

Dieses Schreiben soll die bestehenden Vorgaben in Rz 2.15.1 der W-ISDS bezüglich Verträgen mit Dritten präzisieren.

Ausgangslage und Grundsatz

Für Durchführungsstellen der 1. Säule/FamZ existieren verschiedene Konstellationen mit unterschiedlichen Partnerfirmen für Dienstleistungen im IT und non-IT Bereich. Dabei ist zu beachten, dass die Vorgaben der W-ISDS jeweils für die gesamte Lieferkette Bestand haben. So gelten beispielsweise für den Fall, dass eine Partnerfirma einer Durchführungsstelle der 1. Säule/FamZ ihrerseits einen Dienstleistungsvertrag mit einem oder mehreren Sublieferanten eingeht, die Vorgaben der W-ISDS auch für sämtliche Sublieferanten**.** Dies ist unter anderem der Fall, wenn von einem Dritten Dienstleistungen von einem Public Cloud Provider bezogen werden.

Die untenstehende Grafik verdeutlicht die entsprechenden Verantwortlichkeiten:

Durchführungsstelle 1. Säule/FamZ

- Hat vertragliche Beziehung zu einem IT Provider / IT Pool / externem Dienstleister.
- Verantwortet die Einhaltung der datenschutzrechtlichen Bedingungen gemäss W-ISDS
- Evaluiert datenschutzrechtliche Bestimmungen der Daten, welche durch Externe bearbeitet werden
- Vertragsverhältnis mit Partner entspricht den Vorgaben der W-ISDS

IT Provider / IT Pool / externer Dienstleister

- Hat bei Bedarf vertragliche Beziehung zu einem Sublieferanten oder Provider
- Ist verantwortlich, dass eine vertragliche Beziehung zu einem Sublieferanten den Anforderungen der W-ISDS entspricht (Beispielsweise zusätzliche Verschlüsselung mit eigenem Key bei ausländischen IT-Dienstleistern, Datenhaltung innerhalb der Schweiz etc)

Public Cloud Provider oder IT Dienstleister/Sublieferant

- Muss die vereinbarte Dienstleistung innerhalb der Schweiz erbringen
- Ausländische IT-Dienstleister müssen die Verschlüsselung mit einem vom Kunden kontrollierten Schlüssel für besonders schützenswerte Personendaten unterstützen

Anforderungen und Vorgaben

Im Rahmen von W-ISDS Rz 2.15.1 gelten für Verträge der Durchführungsstellen der 1. Säule/FamZ mit Dritten die folgenden Anforderungen und Vorgaben:

- **Anforderungen an Schutzvorschriften**
  Die Durchführungsstellen der 1. Säule/FamZ müssen den Schutzbedarf der Daten kennen, die sie an Dritte weitergeben wollen. Gegebenenfalls ist eine Risikovorprüfung sowie eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen. Der Schutzbedarf der Daten muss an Vertragspartner (Dritte), welche Zugang zu sozialversicherungsrechtlichen Daten erhalten sollen, kommuniziert werden. Dies ermöglicht den Vertragspartnern, die Einhaltung der Schutzvorschriften frühzeitig zu dokumentieren und den Nachweis zu erbringen, wie sie die Datenschutzvorgaben bezüglich der Daten der Durchführungsstelle einhalten (Grundschutz und allenfalls erweiterte ISDS-Dokumentation).
  Alternativ kann der Datenschutz auch durch eine gültige ISO 27001-Zertifizierung oder einen darauf abgestimmten ISAE 3000-Prüfbericht belegt werden.

- **Sublieferanten**

  Grundsätzlich müssen Verträge mit Dritten vorsehen, dass die vereinbarte Leistung durch den Dritten selbst zu erfüllen ist. Falls Dritte Sublieferanten beiziehen, müssen die Durchführungsstellen der 1. Säule/FamZ als Kunden darüber informiert werden. Dies gilt insbesondere für Dritte, die als Cloud-Reseller auftreten, wie beispielsweise Anbieter von Fachanwendungen im Saas-Modell.

  Bei Auslagerungen an ausländische Sublieferanten oder Verwendung von ausländischen Public Cloud Services, müssen die Vertragspartner der Durchführungsstellen der 1. Säule/FamZ durch geeignete Massnahmen wie zusätzliche eigene Verschlüsselung sicherstellen, dass kein unberechtigter Zugriff (beispielsweise durch den Cloud Provider) auf besonders schützenswerte Personendaten erfolgen kann.

- **Datenbearbeitung im Ausland**

  Die Dienstleistungen für den Betrieb müssen grundsätzlich im Inland erbracht werden. Dienstleistungen für den Betrieb aus dem Ausland sind auszuweisen und zu begründen. Es kommen grundsätzlich nur Länder in Frage, die ein angemessenes Datenschutzniveau ausweisen können. Eine Datenbearbeitung im Ausland ist insbesondere dann möglich, wenn ein lokaler Cloud-Reseller als Vertragspartner der Durchführungsstellen der 1. Säule/FamZ auftritt.

- **Bearbeitung von Personendaten**

  Es muss jederzeit sichergestellt werden, dass keine Personendaten von Versicherten im Ausland bearbeitet werden, ausser es handelt sich um eine Bearbeitung, welche von Gesetzes wegen mit einem internationalen Datenaustausch verbunden ist (z. B. Art. 32 Abs. 3 ATSG, bzw. KSBIL (vgl. Bilaterale Abkommen Schweiz-EU. Abkommen mit der EFTA. Kreisschreiben über das Verfahren zur Leistungsfestsetzung in der AHV/IV)).

  Falls Dritte in der Rolle als Cloud-Reseller Daten bei Public-Cloud-Providern speichern, müssen die folgenden Schutzmassnahmen implementiert werden:

  - Die Daten müssen in einem Rechenzentrum innerhalb der Schweiz bearbeitet werden
  - Zusätzlich müssen entsprechende organisatorische oder technische Massnahmen (Verschlüsselung) implementiert werden, um den Schutz vor unbefugtem Zugriff auf die Daten sicherzustellen

Der Bereich ITM

Für anderweitige Fragen wenden Sie sich an egov@bsv.admin.ch