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. 043 vom 01.01.2022

Geht an:

- Durchführungsstellen der 1. Säule/FamZ

Betreff: Neue Empfehlungen zu den Mindestanforderungen an die Informationssysteme der Durchführungsstellen der 1. Säule/FamZ (Version 1.0:2022)

Die auf der BSV-Vollzugswebseite hier publizierten Empfehlungen richten sich an die Durchführungsstellen der 1. Säule/FamZ. Sie werden publiziert mit Blick darauf, dass voraussichtlich am 1.1.2024 eine AHVG-Gesetzesrevision in Kraft tritt, welche derzeit im Parlament behandelt wird (Botschaft des Bundesrates vom 20. November 2019 zur Modernisierung der Aufsicht in der 1. Säule und Optimierung der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge, Gesetzes-Entwurf BBl 2020 109).

Gestützt auf diese Gesetzesrevision ist damit zu rechnen, dass das Bundesamt für Sozialversicherungen (BSV) Weisungen zu den Mindestanforderungen im Bereich der Informationssicherheit und des Datenschutzes (ISDS) der Informationssysteme (IS) der 1. Säule/FamZ erlassen wird. Mit den vorliegenden Empfehlungen soll bereits im heutigen Zeitpunkt sichergestellt werden, dass sich die Durchführungsstellen (DS) optimal auf die kommenden BSV Weisungen zu den ISDS Mindestanforderungen vorbereiten können. Deshalb wurden die designierten Vertreter der DS (Projekt eAHV/IV Information Security) eng in die Ausarbeitung der vorliegenden Fassung der Empfehlung einbezogen. Am 20.08.2020 wurde im Vorstand eAHV/IV – im Beisein des BSV als Beisitzer - beschlossen, dass ein zweistufiger Review stattfinden soll, Stufe 1 IT der DS, Stufe 2 Review der DS via Verbände. Sprich nach Publikation dieser Version der Empfehlungen findet der Review der Verbände statt, welche bis spätestens Mitte 2022 dazu abschliessend Stellung nehmen.

Bis zum voraussichtlichen Inkrafttreten der AHVG-Gesetzesrevision am 1.1.2024 dürfte auch die bereits beschlossene Revision des Datenschutzgesetzes (nDSG) vom 25. September 2020 (BBl 2020 7639) Geltung haben. Die Verordnungsbestimmungen zum nDSG (nVDSG) sind noch nicht definitiv und werden in einem Zeitpunkt nach Publikation diese Empfehlungen bekannt. Die vorliegenden Empfehlungen berücksichtigen bereits die nDSG Bestimmungen, es muss aber damit gerechnet werden, dass die nVDSG noch inhaltliche Änderungen mit sich bringen können, welche dann in die Weisungen zu den ISDS Mindestanforderungen einfliessen werden. Auch diese Änderungen werden mit den IT Vertretern der DS (Projekt eAHV/IV Information Security) sowie den Verbänden ausgearbeitet und besprochen werden.

Folgende Themen werden insbesondere bei der weiteren Ausarbeitung von Bedeutung sein:

- **ISDS Basis- und erweiterte Dokumentation** (Ziff. 2.8.2 und 2.8.3 bzw. Anhänge 5 und 6): Die Mindestanforderungen müssen auf Kompatibilität mit der neuen nVDSG überprüft werden.

- **Auftrag Dritter/Subunternehmer** (Ziff. 2.15, 2. Bullet): In Bezug auf die Einschaltung von Subunternehmen (Art. 9 Abs. 3 nDSG) ist die Genehmigung des Auftraggebers notwendig.

Diesem gesetzlichen Erfordernis muss auch die kommende Weisung genügen. Die jetzige Empfehlung müsste allenfalls verschärft werden.

- **Auftragsbearbeiter im Ausland** (Ziff. 2.15, 3. Bullet und Anhang 5 Bst. E)**:** Gemäss dieser Empfehlung ist die Datenhaltung grundsätzlich in der Schweiz vorgesehen, und auch die Dienstleistungen für den Betrieb müssen grundsätzlich im Inland erfolgen und Ausnahmen müssen begründet sein. Werden Personendaten von einem Auftragsbearbeiter im Ausland bearbeitet, kommt es zu einer Datenbekanntgabe ins Ausland, und es kommen komplexe Bestimmungen des nDSG zum Tragen. Die Einsetzung eines Dritten als Auftragsbearbeiter im Ausland ist sehr komplex und bedarf äusserst vieler rechtlicher Abklärungen bei Ländern, zu denen der Bundesrat nicht festgestellt hat, dass ein angemessener Schutz gewährleistet ist gemäss Art. 16 Abs. 1 nDSG. In die definitiven Weisungen (Ziff. 2.15) ist ein Hinweis auf die Einschränkungen nach nDSG aufzunehmen, der letztlich für alle DS Geltung haben muss (keine Ausnahmen für kantonale Stellen vorgesehen).

- **Clouddienste Dritter mit Datenhaltung in der Schweiz** (Ziff. 2.15): Es geht hier nicht um eine direkte (Massen-) Datenlieferung – und Auftragsbearbeitung ins Ausland, sondern um die Verletzung des schweizerischen Datenschutzes durch einen in der Schweiz domizilierten Auftragsbearbeitenden. Aktuelles Grundproblem ist die Auftrags-Datenbearbeitung durch Firmen, welche aus Schweizer Sicht dem Schweizer Recht untersteht, jedoch aufgrund des US-amerikanischen Cloud-Acts von amerikanischen Gerichten gezwungen werden kann, bestimmte Daten gegenüber amerikanischen Behörden offen zu legen. Es ist davon, dass ähnliche Probleme auch mit dem Recht anderer Länder bestehen (z.B. China). Grundsätzlich erlaubt die Schweizer Gesetzgebung die Bekanntgabe von Daten im Rahmen einer Strafuntersuchung (vgl. z.B. Art. 50 Abs. 1 Bst. d AHVG). Aufgrund des Territorialprinzips geht die Information aber nur an eine schweizerische Untersuchungsbehörde. Will eine ausländische Untersuchungsbehörde Auskunft, muss sie die Information auf dem Weg der Rechtshilfe – gestützt auf entsprechende internationale Abkommen – einfordern. Die zuständige Schweizer Behörde wird dann an die Durchführungsstelle gelangen. Allerdings erst nach Prüfung des Rechtshilfebegehrens. Rechtshilfebegehren für Straftatbestände, die es nach Schweizer Recht gar nicht gibt, wird nicht stattgegeben. In Bezug auf den Cloud-Act bedeutet dies in der Praxis eine «eigenmächtige Rechtshilfe», so dass das Territorialprinzip ausgeschaltet und das US-amerikanische Straf- Verfahren schneller wird. Der EDÖB kommt in seiner aktuellen Einschätzung[1] und auf der Basis des heute geltenden DSG zu einer eher negativen Beurteilung und hält insbesondere fest: ***«Falls aufgrund der Risikoeinschätzung bezüglich der Verarbeitung von Personendaten in der Cloud Zweifel bestehen, ist von einer Auslagerung der Daten abzusehen.»***

  In der Stellungnahme des EDÖB[2] zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 nDSG vom 8.9.2020 wird ausgeführt, dass bei den US-Zugriffen ein wesentlicher Schutzmechanismus unklar sei und die Grundsätze der rechtmässigen Datenbearbeitung nach DSG verletzt würden. Für die Betroffenen in der Schweiz bei Datenzugriffen von US-Behörden würde es an durchsetzbaren Rechtsansprüchen fehlen, zumal sich die Wirksamkeit des sog. Ombudsperson-Mechanismus, der einen indirekt durchsetzbaren Rechtsbehelf garantieren soll, mangels Transparenz nicht beurteilen lässt und dass die Entscheidkompetenzen der Ombudsperson gegenüber den US-Geheimdiensten sowie ihre tatsächliche Unabhängigkeit ohne hinreichend konkrete und schlüssige Informationen unbelegt bleiben. Dieser Mangel an Transparenz und das daraus abzuleitende Fehlen von Garantien bei Eingriffen der US-Behörden in die Privatsphäre und informationelle Selbstbestimmung von Personen in der Schweiz erachtet der EDÖB als unvereinbar mit dem Anspruch dieser Personen auf einen Rechtsweg nach Art. 29 ff. BV und Art. 15 DSG für die Durchsetzung der ihnen nach Art. 13 Abs. 2 BV sowie Art. 8 EMRK zustehenden Rechte; mit den Grundsätzen einer rechtmässigen Personendatenbearbeitung i.S.v. Art. 4 DSG.
  In der Bundesverwaltung wird derzeit die Problematik der Cloud-Dienste jedoch vertieft geprüft, dies im Rahmen des Projekts «Public Cloud Bund». Bei den Verträgen zwischen dem Bund und

[1] Siehe Erläuterungen zu Cloud Computing (admin.ch)
[2] Siehe Stellungnahme des EDÖB

den fünf Cloud-Anbietern (WTO 20007, Beschaffung Public Cloud Bund) handelt es sich um ein noch laufendes Verfahren. Zuständig ist die Bundeskanzlei. Insofern sollte bis zum Inkrafttreten der BSV ISDS Weisungen eine Ergänzung zum Thema «Aufträgen an Dritten» in Bezug auf Clouddienste möglich sein.

Es lässt sich bereits beim aktuellen Stand des Projekts feststellen, dass Personendaten voraussichtlich nicht in der Cloud von problematischen Anbietern (z.B. Cloud-Act) gespeichert oder anderweitig bearbeitet werden dürfen. Insofern kann die Inanspruchnahme der Clouddienste im Rahmen der Sozialversicherungen in absehbarer Zeit nur empfohlen werden, wenn es sich um Anbieter handelt, welche Gewähr bieten, dass die direkte Herausgabe von Daten an ausländische Behörden ausgeschlossen werden kann.

Wir danken Ihnen für Ihre Kenntnisnahme und die Umsetzung in Ihrer Durchführungsstelle.

Der Bereich ITM

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