Bundesversicherungsamt

Bundesversicherungsamt, Friedrich-Ebert-Allee 38, 53113 Bonn

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1130 / 1151
FAX +49 228 619 1872

referat_116@bvamt.bund.de
www.bundesversicherungsamt.de

BEARBEITER(IN) Fr. Blanke / Hr. Peiffer

14. März 2018

AZ 116 - 820 - 911/2017
(bei Antwort bitte angeben)

An alle
bundesunmittelbaren
Sozialversicherungsträger

- per E-Mail -

nachrichtlich:
Bundesministerium für Arbeit und Soziales
Bundesministerium für Gesundheit
GKV-Spitzenverband
Verband der Ersatzkassen

Wesentliche Anforderungen an Cloud-basierte IT-Lösungen in der Sozialversicherung aus Sicht der Datenverarbeitung und des Datenschutzes

Sehr geehrte Damen und Herren,

mit dem Einsatz von Cloud-Diensten werden im Allgemeinen vielfältige Vorteile verbunden. Durch die gesteigerte Unabhängigkeit von eigenen IT-Ressourcen und Geschäftsprozessen, stellen sich die Vorteile der Integration von Cloud-Technologien unter anderem in Form von gesteigerter Flexibilität und Kostenersparnissen durch bessere Skalierbarkeit dar.

Dem gegenüber sind als Nachteile insbesondere strategische Abhängigkeiten von externen Cloud-Anbietern sowie eine prinzipiell höhere Gefahr hinsichtlich des Verlusts der Vertraulichkeit extern verarbeiteter Sozialdaten oder beispielsweise deren Revisionssicherheit.

Im Rahmen einer detaillierten Analyse, ob Cloud-basierte IT-Lösungen eine vorteilhafte Alternative darstellen, sind insbesondere folgende Grundanforderungen zu berücksichtigen:

- Der Einsatz von Cloud-Diensten ist nur zur Erfüllung eigener gesetzlicher Aufgaben zulässig (§ 30 SGB IV).

- Sofern Sozialdaten in externen Cloud-Lösungen verarbeitet werden sollen, kann dies nur auf Grundlage einer Auftragsdatenverarbeitung erfolgen (§ 80 SGB X, ab dem 25. Mai 2018 i. V. m. Artikel 28 DSGVO).
- Im Rahmen einer Auftragsdatenverarbeitung sind insbesondere die gesetzlich vorgegebenen Regelungsaspekte wirksam mit dem Auftragnehmer zu vereinbaren (§ 80 Abs. 2 SGB X bzw. ab dem 25. Mai 2018 Artikel 28 Abs. 3 DSGVO i. V. m. dem Erwägungsgrund 81 und § 80 SGB X n. F.). Je nach Gestaltung der Vereinbarung müssen dabei auch vertraglich in Bezug genommene Unterlagen (z. B. Service-Bedingungen) vor dem Hintergrund der Anforderungen bewertet werden.
- Die Einbeziehung externer Cloud-Dienste muss in der allgemeinen Sicherheitskonzeption berücksichtigt werden. Es sind geeignete Schutzmaßnahmen zu treffen, die im Verhältnis zum jeweils ermittelten Schutzzweck angemessen sind (§ 78a SGB X bzw. ab dem 25. Mai 2018 Artikel 32 DSGVO i. V. m. Erwägungsgrund 83). Hier können auch weitere Anforderungen an die Sicherheitskonzeption (z. B. gemäß BSI-Gesetz) einschlägig sein.
- Bei einer geplanten Verarbeitung von Sozialdaten außerhalb der Europäischen Union (z. B. durch einen administrativen Zugriff aus einem Drittland) muss ab dem 25. Mai 2018 explizit geprüft werden, ob die besonderen Anforderungen an eine solche Verarbeitung erfüllt werden (Artikel 44 ff. DSGVO i. V. m. Erwägungsgründe 101 ff.) und ob insbesondere auch hier hinreichende Garantien für den Schutz der personenbezogenen Daten gegeben werden können (Artikel 28 DSGVO i. V. m. Erwägungsgrund 81).
- Für eine Verarbeitung besonderer Arten personenbezogener Daten (§ 67 Abs. 12 SGB X) bzw. ab dem 25. Mai 2018 besonderer Kategorien personenbezogener Daten (Artikel 9 Abs. 1 DSGVO) sind besondere Schutzmaßnahmen auf Grundlage einer eigenen Risikoanalyse zu treffen (Artikel 32 Abs. 2 DSGVO i. V. m. Erwägungsgrund 83).
- Soweit eine Nutzung externer Cloud-Dienste aus sozial- und datenschutzrechtlicher Sicht zulässig ist, muss insbesondere vor dem Hintergrund der eingangs erwähnten strategischen Abhängigkeit eine Wirtschaftlichkeitsanalyse erfolgen (§ 69 Abs. 2 SGB IV). Dabei sollten insbesondere ein Vergleich mit anderen Cloud-Konzepten (z. B. private Cloud) angestellt sowie die strategischen Abhängigkeiten (sog. Lock-In-Effekte) analysiert werden.

Die vorgenannten Punkte sollen eine erste Orientierung bieten. Es handelt sich um wesentliche Anforderungen, die wir im Rahmen unserer Aufsichtstätigkeit vielfach mit Trägern diskutiert haben. Wir erheben keinen Anspruch auf Vollständigkeit.

Als eine weitere methodische Unterstützung einer ersten Orientierung haben wir diesem Rundschreiben als Anhang ein grobes initiales Prüfschema aus dem Blickwinkel der Datenverarbeitung und des Datenschutzes beigefügt. Weitere gesetzliche Anforderungen, wie z. B. verfahrensrechtliche Formerfordernisse, Vorgaben bezüglich der Beschaffung, Vergabe oder der Finanzierung, werden hierbei nicht berücksichtigt.

Für eine detaillierte Befassung mit der datenschutzrechtlichen Thematik verweisen wir u. a. auf die „Orientierungshilfe – Cloud Computing" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Version 2.0, Stand 09.10.2014).[1]

Für eine detaillierte Befassung mit den Aspekten der Informationssicherheit verweisen wir insbesondere auf den Anforderungskatalog Cloud Computing (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI)[2] bzw. auf die Mindeststandards zur Nutzung externer Cloud-Dienste des BSI.[3]

Das Bundesversicherungsamt wird den Einsatz von Cloud-Lösungen, insbesondere vor dem Hintergrund der dargestellten Anforderungen, sukzessive überprüfen.

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)

---

[1] Vgl. u. a. https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/orientierungshilfen-node.html (letzter Zugriff: 28.11.2017).

[2] Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/CloudComputing_ node.html (letzter Zugriff: 28.11.2017).

[3] Https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_ Nutzung_externer_Cloud-Dienste.pdf?__blob=publicationFile&v=7 (letzter Zugriff: 28.11.2017).

Prüfschema zur Beurteilung der datenschutzrechtlichen Zulässigkeit der Nutzung externer Cloud-Dienste bei der Verarbeitung von Sozialdaten