Bundesversicherungsamt

Bundesversicherungsamt, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Sozialversicherungsträger

- per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

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

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

BEARBEITER(IN) Hr. Peiffer

22. März 2019

AZ 116 - 835 - 2711/2017
(bei Antwort bitte angeben)

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 Informationstechnik und des Datenschutzes

Aktualisierung unseres Rundschreibens vom 14. März 2018

Sehr geehrte Damen und Herren,

aufgrund neuer Erkenntnisse aus unserer Aufsichtsführung aktualisieren wir unser Rundschreiben zu den wesentlichen Anforderungen an Cloud-basierte IT-Lösungen in der Sozialversicherung. Um die Lesbarkeit zu vereinfachen, enthalten die folgenden Hinweise die weiterhin gültigen Aussagen unseres o. a. Rundschreibens. Dieses kann somit vollständig ausgetauscht werden.

Mit dem Einsatz von Cloud-Diensten werden in der Regel bedarfsgerechte Zugriffe auf Informationstechnologien (z. B. Hardware, Software, Plattformen) in Form von Services über Netzwerk verbunden (in der Regel Internet oder Intranet).[1] Als zentraler Vorteil wird hierbei

[1] Vgl. u. a. Heinrich et al.: Informationsmanagement, 11. Auflage, Oldenbourg-Verlag, München 2014, S. 39.

oftmals die Unabhängigkeit von eigenen IT-Ressourcen angeführt, welche zum einen die flexible Realisierung neuer Geschäftsprozesse ermöglicht und zum anderen Kostenersparnisse durch eine bessere Skalierbarkeit bedingt. Demgegenüber sind als Nachteile insbesondere strategische Abhängigkeiten von externen Anbietern sowie eine prinzipiell höhere Gefahr des Verlusts der Vertraulichkeit extern verarbeiteter Daten abzuwägen.

Vor diesem allgemeinen Hintergrund sind im Rahmen einer detaillierten Analyse, ob Cloud-basierte IT-Lösungen eine vorteilhafte Alternative darstellen, insbesondere folgende Grundanforderungen zu berücksichtigen:

a) Aufgabenbezug

Der Einsatz von Cloud-Diensten ist nur zur Erfüllung eigener gesetzlicher Aufgaben zulässig (§ 30 SGB IV). Die konkreten Verarbeitungsbefugnisse müssen sich direkt aus den jeweiligen Sozialgesetzbüchern (im Folgenden kurz: SGB) ergeben. Die Zwecke der Verarbeitung und die korrespondierende gesetzliche Grundlage sind ebenfalls Ausgangspunkt einer etwaigen Datenschutz-Folgenabschätzung gemäß Artikel 35 der EU-Datenschutzgrundverordnung (im Folgenden kurz: DSGVO).

b) Vereinbarung einer Auftragsverarbeitung gemäß Artikel 28 DSGVO

Sofern personenbezogene Daten durch Cloud-Anbieter verarbeitet werden, liegt datenschutzrechtlich in der Regel eine Auftragsverarbeitung vor. Üblicherweise tritt dabei der jeweilige Sozialversicherungsträger als Verantwortlicher und der Cloud-Anbieter als Auftragsverarbeiter auf. Somit ist der Abschluss einer Vereinbarung gemäß Artikel 28 DSGVO erforderlich. Dabei sind sowohl formelle (vgl. Artikel 28 Absatz 3 Satz 1) als auch inhaltliche (vgl. Artikel 28 Absatz 3 Satz 2) Anforderungen zu erfüllen.

Hierbei können einer wirksamen Vereinbarung zwar grundsätzlich auch vorformulierte Vereinbarungstexte in Form von Mustern zugrunde gelegt werden. Ein bloßer Verweis auf Allgemeine Geschäftsbedingungen genügt den gesetzlichen Anforderungen aber nicht. Für unzulässig halten wir auch Vereinbarungen, die unbestimmte und sehr allgemein gehaltene Regelungen enthalten oder einseitige Anpassungs- oder Änderungsmöglichkeiten des jeweiligen Anbieters vorsehen. Wir weisen darauf hin, dass eine wirksame Vereinbarung insbesondere das konkrete Verarbeitungsszenario zutreffend abbilden und einen dauerhaften Rechtsbindungswillen des Cloud-Anbieters erkennen lassen muss. Sofern Zweifel bestehen, ob die durch den Cloud-Anbieter zur Verfügung gestellten Vereinbarungen diesen Anforde-

rungen genügen, empfehlen wir, die Vereinbarung in Anlehnung an einschlägige Muster (z. B. des vdek e. V. bzw. des GKV-Spitzenverbandes) auszugestalten.

c) Besonderheiten des Sozialdatenschutzes gemäß § 80 SGB X

Sofern im Rahmen einer Cloud-Lösung Sozialdaten verarbeitet werden, sind über die allgemeinen Anforderungen des Artikels 28 DSGVO hinaus die besonderen Maßgaben des § 80 SGB X zu beachten. Insbesondere darf ein Auftrag zur Verarbeitung von Sozialdaten gemäß § 80 Absatz 2 SGB X nur erteilt werden, wenn die Verarbeitung

- im Inland,
- in einem anderen Mitgliedstaat der Europäischen Union,
- in einem sog. gleichgestellten Staat (§ 35 Absatz 7 SGB I) oder
- in einem Drittstaat oder in einer internationalen Organisation erfolgt, sofern ein Angemessenheitsbeschluss der EU-Kommission gemäß Artikel 45 DSGVO vorliegt.

Diese Regelung hat der Gesetzgeber im Rahmen der Anpassung des SGB I und X an die DSGVO aufgenommen. In der Gesetzesbegründung wurde deutlich gemacht, dass es bei der Verarbeitung von Sozialdaten aufgrund des regelmäßig besonders hohen Schutzbedarfs eine räumliche Beschränkung der Verarbeitung geben soll (vgl. BT-Drs. 18/12611, S. 114). Die in Artikel 46 DSGVO dargestellten „geeigneten Garantien" stellen hingegen keine zulässigen Rechtsgrundlagen für die Verarbeitung von Sozialdaten in Drittstaaten dar. Die weit verbreiteten Standardvertragsklauseln (Absatz 2 lit. c und d) können hier daher ebenso wenig legitimierend herangezogen werden wie die sog. Binding Corporate Rules (Absatz 2 lit. b) und die genehmigten Verhaltensregeln (Absatz 2 lit. e und f).

Diese Beschränkung erstreckt sich nicht nur auf den Speicherort „ruhender" Sozialdaten, sondern erfasst grundsätzlich sämtliche Verarbeitungssituationen. Selbst wenn im Rahmen eines Vorhabens also etwa Sozialdaten in deutschen oder europäischen Rechenzentren gespeichert werden, müssen insbesondere Wartungs- und Supportabläufe vor dem Hintergrund der gesetzlichen Regelungen differenziert betrachtet werden. Regelmäßig führen Anbieter ihre Geschäftsprozesse global nach dem sog. „Follow-the-sun"-Prinzip aus. In unserer Aufsichtspraxis standen hier insbesondere Supportzugriffe aufgrund von Kundenanfragen sowie infrastrukturelle Verfahren zum Schutz vor Schadsoftware und zur Analyse von Systemabbrüchen und -fehlern im Fokus der Prüfung. Im Sinne einer rechtskonformen Verarbeitung ist hier regelmäßig eine zusätzliche Vereinbarung von technischen und organisatorischen Maßnahmen zur Vermeidung einer unbefugten Verarbeitung von Sozialdaten erforderlich.

So können Supportzugriffe aus unzulässigen Drittstaaten beispielsweise verhindert werden, indem feste Support-Manager oder eine festgelegte Supportregion vereinbart werden. Als geeignet sehen wir auch Freigabeverfahren für Wartungszugriffe an, bei denen der verantwortliche Träger selbst Zugriffsanfragen genehmigen oder auch abweisen kann.

Hinsichtlich weitgehend automatisierter Abläufe, zum Beispiel zum Schutz vor Schadsoftware, ist die Gestaltung des jeweiligen Prozesses für die datenschutzrechtliche Beurteilung relevant. Soweit eine kurzzeitige Prüfung auf Schadcode in einer sicheren Umgebung in einem geschützten, automatisierten Prozess stattfindet und z. B. Administratorenzugriffe begrenzt und nachvollziehbar dokumentiert werden, halten wir dies für tolerierbar. Diese Anforderungen gelten in gleicher Weise auch für Analysen von Systemfehlern, bei denen automatisiert Speicherabbilder gesichert und ausgewertet werden. Auch hier müssen im Einzelfall der konkrete Prozess analysiert und die besonderen Sicherheitsmaßnahmen aus datenschutzrechtlicher Sicht bewertet werden.

d) Auswirkungen auf die Sicherheitskonzeption

Die Einbeziehung externer Cloud-Dienste muss in der allgemeinen Sicherheitskonzeption berücksichtigt werden. Auf Basis einer Risikoanalyse sind hierbei regelmäßig geeignete Schutzmaßnahmen zu treffen, die im Verhältnis zum ermittelten Schutzzweck angemessen sind (Artikel 32 DSGVO i. V. m. Erwägungsgrund 83). Hier können auch weitere Anforderungen an die Sicherheitskonzeption (z. B. gemäß BSI-Gesetz) einschlägig sein.

Im Zusammenhang mit der Nutzung von Cloud-Diensten kommt insbesondere der Verschlüsselung von Daten eine herausgehobene Bedeutung zu. Bei der Bewertung eines konkreten Verfahrens sind hier jedoch nicht nur die kryptographischen Spezifikationen einer Lösung ausschlaggebend, sondern auch deren Implementierung in die betrieblichen Abläufe. Vor dem Hintergrund der Wahrung der Vertraulichkeit sind insbesondere die verschiedenen Verschlüsselungskonzepte (Inhalts-, Dienste- und / oder Festplattenverschlüsselung) wichtige Aspekte einer Einzelfallprüfung. Diese Betrachtung sollte sich nicht auf die integrierten Lösungsansätze der jeweiligen Cloud-Lösungen beschränken, sondern auch weitergehende Maßnahmen (z. B. die Verwendung eigener kryptographischer Schlüssel oder die Implementierung zusätzlicher, kundenseitiger Verschlüsselungsmaßnahmen) einbeziehen.

e) Berücksichtigung und Bewertung ökonomischer Effekte

Soweit eine Nutzung externer Cloud-Dienste aus sozial- und datenschutzrechtlicher Sicht zulässig ist, müssen die ökonomischen und meist strategischen Effekte umfassend analysiert werden (§ 69 Absatz 2 SGB IV).

Als Vorteile werden häufig die Unabhängigkeit von eigenen IT-Ressourcen, die dadurch erzielte Flexibilität bei der (agilen) Anpassung von Geschäftsprozessen sowie Kostenersparnisse durch bessere Skalierbarkeit genannt. Diese Argumente sind im Rahmen der Wirtschaftlichkeitsbetrachtung nicht zuletzt im Hinblick auf spätere Erfolgskontrollen mit Fakten zu untermauern. In der Fachöffentlichkeit konnte nachverfolgt werden, dass die ökonomischen Vorteile aufgrund unerwarteter Zusatzkosten nicht in allen Fällen realisiert werden konnten und nachträgliche Analysen häufig zugunsten einer sog. On-Premises-Lösung, also der Bereitstellung des jeweiligen Dienstes aus dem eigenen Rechenzentrum, ausfallen.[2]

Als Nachteile sind insbesondere strategische Abhängigkeiten von externen Cloud-Anbietern und sog. Lock-in-Effekte zu berücksichtigen: Bei zunehmender Integration der Cloud-Dienste in das Informationssystem werden die Wechselkosten erhöht, was zur sinkenden Wahrscheinlichkeit eines Systemwechsels führt. Diese negativen Effekte sind zu berücksichtigen, indem einerseits die Wechselkosten mit kalkuliert und andererseits Exit-Strategien entwickelt werden (z. B. sog. Multi-Cloud-Ansätze, um die Abhängigkeit von einigen wenigen Anbietern zu reduzieren und / oder sog. Hybrid-Cloud-Ansätze, um besonders kritische Daten weiterhin selbst zu speichern).

Nicht zuletzt ist die Außenwirkung der Verarbeitung von Sozialdaten in der Cloud zu berücksichtigen. Auch wenn die rechtlichen und sicherheitstechnischen Voraussetzungen erfüllt sind, hängt in manchen Anwendungsbereichen der positive Veränderungsprozess bei der Einführung digitaler Lösungen von der Akzeptanz und dem (subjektiven) Vertrauen der Versicherten ab. Dies muss ebenfalls berücksichtigt werden.

Im Ergebnis ist der Einsatz von Cloud-Technologien und Lösungen auch in der Sozialversicherung möglich, soweit die besonderen Vorgaben des Sozialdatenschutzes berücksichtigt werden. Die vorgenannten Punkte sollen für die eigenen Prüfungen eine erste Orientierung geben und zum Problembewusstsein beitragen. Auf dieser abstrakten Ebene ist es aber nicht möglich, auf alle einzelfallbezogenen Aspekte einzugehen. Insoweit erheben wir keinen

[2] Vgl. hierzu u. a. https://heise.de/-4072912, letzter Zugriff: 16.03.2019.

Anspruch auf Vollständigkeit. Zudem haben wir in unserer Darstellung bewusst Problemfelder ausgeblendet, welche sich auch unabhängig von der Verwendung von Cloud-Diensten ergeben (z. B. die Zulässigkeit der Übermittlung sog. Telemetriedaten). Auch weitere gesetzliche Anforderungen, wie z. B. verfahrensrechtliche Formerfordernisse, Vorgaben bezüglich der Beschaffung, der Vergabe oder der Finanzierung, waren nicht Gegenstand unserer Ausführungen und sind im Einzelfall von der verantwortlichen Stelle selbstständig zu berücksichtigen.

In Übereinstimmung mit unserem gesetzlichen Auftrag unterstützen wir die Institutionen in unserem Aufsichtsbereich gerne bei der Planung und Umsetzung individueller Vorhaben. Leider wird uns immer wieder berichtet, dass einzelne Anbieter behaupten, ein bestimmtes Produkt oder eine bestimmte Lösung sei durch das Bundesversicherungsamt freigegeben oder zertifiziert. Dies ist nicht zutreffend. Wir treffen keine grundsätzlichen Güteaussagen zu bestimmten Anbietern oder Produkten.

Für eine weitergehende 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).[3]

Für eine weitergehende Befassung mit den Aspekten der Informationssicherheit verweisen wir insbesondere auf den Anforderungskatalog Cloud Computing (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI).[4]

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)

---

[3] Vgl. u. a. https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/orientierungshilfen-node.html (letzter Zugriff: 19.03.2019).

[4] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.html (letzter Zugriff: 19.03.2019).