Bundesamt
für Soziale Sicherung

Bundesamt für Soziale Sicherung, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Sozialversicherungsträger

- per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1833 / 1154

Referat116@bas.bund.de
www.bundesamtsozialesicherung.de

BEARBEITER(IN) HR. ZIEHMS / HR. SECK

21. Oktober 2021

AZ **116 - 830 - 3395/2020**
(bei Antwort bitte angeben)

Informationstechnik im Aufsichtsbereich – hier: Wesentliche Anforderungen an den sicheren Einsatz mobiler Applikationen in der Sozialversicherung

Sehr geehrte Damen und Herren,

im Rahmen der digitalen Veränderungsprozesse in der Sozialversicherung wird eine kontinuierlich wachsende Anzahl an Leistungen und Funktionen über mobile Anwendungen bzw. Applikationen (kurz: Apps) bereitgestellt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert eine App grundsätzlich als ein Programm, das auf einer mobilen Plattform ausgeführt wird. Der Betrieb einer solchen App kann dabei autonom auf dem Endgerät oder in Kombination mit einem sicheren Backend betrieben werden.[1]

Im Gegensatz zu den Digitalen Gesundheitsanwendungen, bei denen der Gesetzgeber in den §§ 33a und 139e SGB V sowohl den Anspruch auf die Bereitstellung als auch ein Antrags- und Prüfverfahren festgelegt hat, sind Anforderungen an den Einsatz von Service- oder Geschäftsstellen-Apps nicht explizit gesetzlich zusammengefasst. Dabei sind neben technischen Anforderungen bei der Entwicklung und dem sicheren Einsatz entsprechender Apps oft zusätzliche komplexe Herausforderungen zu berücksichtigen, die sich beispielsweise auch aus der Nutzung von Cloud-Diensten oder durch Analyse der App-Nutzung mittels Tracking-Diensten ergeben.

---

[1] Vgl. hierzu die Technische Richtlinie TR-03161 des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Stand: 15.04.2020, S. 6 und 8 und das IT-Grundschutz-Kompendium des BSI, Stand Februar 2021, Baustein APP.1.4.

Mit dem vorliegenden Rundschreiben wollen wir einen Beitrag dazu leisten, die grundlegenden rechtlichen und technischen Anforderungen für den Einsatz von mobilen Applikationen in der Sozialversicherung in systematischer Weise darzustellen.

Wir orientieren uns dabei an dem im IT-Grundschutz-Kompendium des (BSI) dargestellten Lebenszyklusmodell. Danach durchläuft jegliche Software einen Lebenszyklus, der die Planung, Anforderungserhebung, Beschaffung, Software-Tests inklusive Freigabe, Installation in Produktivumgebung, Schulung, Betrieb, Updates und Änderungsmanagement sowie Außerbetriebnahme und Deinstallation umfasst. Je nach Anwendungskontext können dabei einzelne Aspekte dieses Lebenszyklus variieren.[2]

Die rechtlichen Anforderungen für einen Einsatz von mobilen Applikationen in der Sozialversicherung haben wir entsprechend der folgenden Lebenszyklus-Phasen strukturiert:

1. Konzeption - umfasst die Planung und Anforderungserhebung
2. Beauftragung
3. Implementierung
4. Software-Tests inklusive Freigabe
5. Betrieb
6. Laufende Evaluierung - umfasst Updates und Änderungsmanagement

Wir werden im Folgenden die aus unserer Sicht relevanten Anforderungen im Rahmen dieses App-Lebenszyklus darstellen:

1. Konzeption

Unter Berücksichtigung der rechtlichen Anforderungen sind bei der Konzeption von Apps insbesondere folgende Aspekte zu beachten:

1.1 Rechtsgrundlage der Verarbeitung

Der Zweck der Datenverarbeitung in der App muss sich direkt aus entsprechenden gesetzlichen Aufgaben innerhalb der jeweiligen Sozialgesetzbücher ergeben (vgl. § 30 SGB IV).

---

[2] Vgl. hierzu das IT-Grundschutz-Kompendium des BSI, Baustein APP.6: Allgemeine Software, Nr. 1.1, Stand Februar 2021.

1.2 Integration in das bestehende Datenschutz- und Sicherheitskonzept

Gemäß Artikel 32 Absatz 1 der Datenschutz-Grundverordnung (DSGVO) haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei ist der Stand der Technik und der Zweck der Verarbeitung zu berücksichtigen und unter Abwägung des Risikos für die Rechte und Freiheiten der Betroffenen ein angemessenes Schutzniveau zu gewährleisten.

Schon während der Konzeption sollte die App in die allgemeine Datenschutz- und Sicherheitskonzeption integriert werden. Geeignete Schutzmaßnahmen sind in Relation zu dem ermittelten Schutzzweck anzuwenden. Insbesondere die datenschutzrechtliche Verantwortlichkeit der Verarbeitung muss eindeutig geregelt sein.

1.3 Auftragsverarbeitung bei der Nutzung von Cloud-Diensten

Werden personenbezogene Daten von Dritten (z. B. durch einen Cloud-Anbieter) verarbeitet, liegt in der Regel eine Auftragsverarbeitung vor, für die der Abschluss einer Vereinbarung gemäß Artikel 28 DSGVO erforderlich ist. Sofern in diesem Rahmen Sozialdaten verarbeitet werden, sind darüber hinaus die spezifischen Maßgaben des § 80 SGB X zu berücksichtigen.

Der Abschluss einer Vereinbarung über die Verarbeitung im Auftrag ist grundlegende Voraussetzung für einen rechtskonformen Einsatz von Cloud-Diensten, sofern personenbezogene Daten durch den Cloud-Anbieter verarbeitet werden. Darüber hinaus muss sichergestellt werden, dass die Verarbeitung nur im Inland, einem Mitgliedstaat der Europäischen Union oder einem Drittland, in dem ein angemessenes Schutzniveau gewährleistet ist, erfolgt (vgl. § 80 Abs. 2 SGB X). Wir verweisen in diesem Kontext auch auf unser Rundschreiben zu den Anforderungen an Cloud-basierte IT-Lösungen in der gesetzlichen Sozialversicherung vom 22. März 2019.[3]

---

[3] Vgl. hierzu https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20190322Cloud-Computing-in-der-SV.pdf (letzter Zugriff: 05.10.2021).

2. Beauftragung

Wird die App nicht selbstständig durch den Sozialversicherungsträger programmiert, sondern individuell beauftragt, muss sichergestellt werden, dass die in der Konzeptionsphase betrachteten rechtlichen Anforderungen durch den Auftragnehmer eingehalten werden. Dies gilt ebenfalls, wenn eine sogenannte „White-Label App" bei einem darauf spezialisierten Anbieter beauftragt wird und für die Bereitstellung der für den Betrieb der App erforderlichen Backend-Dienste.

Im Folgenden stellen wir weitere grundlegende Aspekte dar, die bei der Beauftragung einer App und der dafür erforderlichen Backend-Dienste zu beachten sind.

2.1 Berücksichtigung rechtlicher Anforderungen im Rahmen der Dienstleistersteuerung

Bei Beauftragung externer Dienstleister für die Umsetzung von App-Funktionalitäten ist die Einhaltung datenschutzrechtlicher Anforderungen durch den Auftragnehmer seitens des Auftraggebers sicherzustellen. Die Rechtmäßigkeit der Datenverarbeitung sowie die Integration in die allgemeine Sicherheitskonzeption des Sozialversicherungsträgers sind auch bei einer Auftragsfertigung zu berücksichtigen. Dies kann z. B. dadurch erfolgen, dass die Entwicklung der App im Rahmen eines Projektes des beauftragenden Sozialversicherungsträgers erfolgt und somit auch eng begleitet wird. In diesem Entwicklungsprojekt sind dann auch die Sicherheitsmechanismen und datenschutzrechtlichen Anforderungen an die Entwicklung der App sowie die Verantwortlichkeiten für die Steuerung des externen Dienstleisters festzulegen. Der umfassenden Dokumentation der Anforderungen kommt dabei eine wesentliche Bedeutung zu.

2.2 Nutzung von Backend-Ressourcen

Neben den datenschutzrechtlichen Anforderungen sind bei der Anbindung von Backend-Diensten auch regelmäßig technische Aspekte in die Betrachtung einzubeziehen. Hier sind insbesondere die Kommunikationsschnittstellen zwischen der App und den Backend-Diensten aber auch die Kommunikationsschnittstellen zwischen einzelnen Komponenten zur Sicherstellung von Authentizität, Integrität und Vertraulichkeit in der Sicherheitskonzeption zu berücksichtigen.[4]

---

[4] Vgl. IT-Grundschutz-Kompendium, APP.1.4, Nr. 2.8.

Im Kontext mobiler Apps liegt ein besonderer Fokus auf der Auswahl geeigneter kryptografischer Maßnahmen, um eine sichere Verbindung zwischen App und Backend zu gewährleisten. Dies bedeutet, dass zum einen die Daten zwischen App und Backend sowohl vor dem Auslesen durch Dritte geschützt sind und zum anderen auch ein Schutz vor der Manipulation des Datenverkehrs besteht. Ein zusätzlicher Nutzen besteht beispielsweise darin, dass zwischen App und Backend eine digitale Vertrauensbasis hergestellt werden kann, die verhindert, dass Daten weder von noch an ein manipuliertes Backend übertragen werden.

2.3 Einbindung von Tracking-Diensten

Verfahren, die Daten für technische Aspekte des Webseitenbetriebs oder zur Analyse des Nutzerverhaltens erheben, werden im Kontext dieses Rundschreibens als Tracking-Dienste bezeichnet. Basierend auf Erkenntnissen aus unserer Aufsichtstätigkeit werden zur Analyse des Nutzungsverhaltens häufig Tracking-Dienste von Drittanbietern in eine App eingebunden. Hier sollte im Zweifelsfall davon ausgegangen werden, dass personenbezogene Daten, wie die IP-Adresse des Nutzers, in den erhobenen Analysedaten vorhanden sind, sodass auch hierfür die datenschutzrechtlichen Maßgaben der DSGVO und der Sozialgesetzgebung zur Anwendung kommen.

Für eine rechtskonforme Einbindung von Tracking-Diensten durch Dritte ist zunächst die Rechtmäßigkeit der Verarbeitung der Daten sicherzustellen, z. B. durch Einwilligung der Betroffenen oder Begründung eines berechtigten Interesses. Ebenso ist die Rechtsgrundlage für die Einbindung Dritter, in der Regel im Rahmen einer Verarbeitung im Auftrag nach Artikel 28 DSGVO oder in Form einer gemeinsamen Verantwortung gemäß Artikel 26 DSGVO erforderlich. Darüber hinaus ist die Einwilligung in die Analyse des Nutzungsverhalten datenschutzkonform zu gestalten. Dabei ist zu beachten, dass nach Artikel 12 DSGVO alle Informationen in präziser, transparenter und leicht zugänglicher Form zu übermitteln sind. Konkrete Anforderungen über Informationen, die Verantwortliche bei der Erhebung personenbezogener Daten zur Verfügung stellen müssen, sind in Artikel 13 und 14 DSGVO dargestellt. Neben diesen grundsätzlichen datenschutzrechtlichen Anforderungen können sich bei der Umsetzung weitere verbraucherrechtliche Informationspflichten über die Funktionsweise digitaler Inhalte ergeben, die im Rahmen dieses Rundschreibens nicht detailliert behandelt werden.[5]

---

[5] Eine gute und aktuelle Zusammenfassung der Anforderungen sowie der verbraucher- und datenschutzrechtlichen Problemfelder bietet auch die „Sektoruntersuchung Mobile Apps“ des Bundeskartellamts, Juli 2021,

3. Implementierung

Im Hinblick auf die Einhaltung der Schutzziele Integrität, Vertraulichkeit, Verbindlichkeit und Authentizität bei der Programmierung einer App fordert Artikel 32 DSGVO durch den Verantwortlichen und den Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen. Hierzu ist es unabdingbar, diese Schutzziele auch bei der Implementierung einer App zu berücksichtigen. Darüber hinaus können sich aus dem geplanten Einsatzzweck auch weitergehende Anforderungen ergeben, z. B. bei der Entwicklung von digitalen Gesundheitsanwendungen im Sinne des § 33a SGB V oder Anwendungen, die unter die Richtlinie des GKV-Spitzenverbands zu § 217f Abs. 4b SGB V fallen.

Neben Vorgaben für funktionale Anforderungen sind bereits in der Implementierungs-Phase Aspekte der Codequalität und der sicheren Programmierung in die Betrachtung mit einzubeziehen. Als Orientierungshilfe, um eine in Bezug auf die Informationssicherheit dem Stand der Technik entsprechende Implementierung zu erreichen, können - abhängig vom Einsatzzweck der App – die folgenden Standards und Richtlinien als Referenz herangezogen werden:

3.1 Allgemeine Richtlinien für die Implementierung einer App

Im Hinblick auf die sichere Programmierung von Apps empfehlen wir, die Vorgaben und Empfehlungen der BSI TR-03161 - soweit anwendbar - umzusetzen. Zusätzlich empfehlen wir unabhängig vom geplanten Einsatzzweck die Orientierung an internationalen Standards, wie z.B. den „Smartphone Secure Development Guidelines“[6], dem „Mobile AppSec Verification Standard“ und dem damit verbundenen „Mobile Security Testing Guide“[7] sowie den weiteren Hinweisen des Open Web Application Security Project (OWASP)[8].

3.2 Spezifische Standards der Sozialversicherungsträger

Je nach Einsatzzweck der App ist durch den Auftraggeber zu prüfen, ob bei der Entwicklung der App zusätzliche technische Vorgaben, wie z. B. die Verwendung von bestimmten

---

https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Mobile_Apps.pdf, Abschnitt III, Seite 50 ff.

[6] Vgl. https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016, letzter Zugriff: 05.10.2021.

[7] Vgl. https://owasp.org/www-project-mobile-security-testing-guide/, letzter Zugriff: 05.10.2021.

[8] Vgl. https://owasp.org/www-project-application-security-verification-standard/, letzter Zugriff: 05.10.2021.

Authentifizierungsverfahren oder die Sicherstellung einer verschlüsselten Datenübertragung einzuhalten sind. Diese ergeben sich zum Beispiel bei denjenigen Apps, die unter die Richtline des GKV-Spitzenverbands zu § 217f Abs. 4b SGB V fallen.

4. Software-Tests und Freigabe

Vor dem Veröffentlichen der App ist diese im Rahmen eines vorher festgelegten Testverfahrens darauf zu überprüfen, ob die Anforderungen an die Funktionalität, den Datenschutz und die Datensicherheit eingehalten werden. Wir empfehlen, das Testverfahren an den Anforderungen des Bausteins OPS.1.1.6 des IT-Grundschutz-Kompendiums zu orientieren und sowohl die Beauftragten für den Datenschutz als auch der Informationssicherheit in dieses Verfahren einzubinden.

Wir halten es dabei für wesentlich, im Vorfeld die Verantwortlichkeiten für das Festlegen der Rahmenbedingungen, die Durchführung der Tests, das Auswerten der Testergebnisse und die Freigabe der App festzulegen.

Die Testanforderungen sind zudem regelmäßig an Änderungen im technischen Umfeld, beispielsweise im Bereich der Kryptographie, anzupassen. Auch im Hinblick auf die Prüfung von Sicherheitsaspekten sollten die Testanforderungen im Hinblick auf neu erkannte Schwachstellen regelmäßig überprüft und angepasst werden. Einen Anhaltspunkt für die Fortentwicklung liefern die regelmäßig fortgeschriebenen Auswertungen des OWASP-Projekts zu den zehn häufigsten Schwachstellen von Webanwendungen („OWASP Top 10“[9]).

Die App und die für den Betrieb erforderlichen Backend-Dienste sollten nur in einer separaten Testumgebung getestet werden. Für den Umgang mit der Testumgebung nach Abschluss der Tests sollten Verfahren definiert sein, die beispielsweise die Löschung von Testdaten und den Zugang zur Testumgebung regeln.

Da bei einer Verarbeitung von Sozialdaten üblicherweise ein hoher Schutzbedarf anzunehmen ist, sollte entsprechend den Empfehlungen des BSI die Durchführung von Penetrationstests vor der Freigabe der App eingeplant werden.

---

[9] Siehe hierzu https://owasp.org/Top10/ (letzter Zugriff: 05.10.2021).

5. Betrieb

Die App und die für den Betrieb erforderlichen Backend-Dienste müssen wie oben dargestellt in ein Datenschutz- und Sicherheitskonzept integriert sein. Die Verantwortlichkeiten für die Prüfung der App und der Umgang mit Störungen und Sicherheitsvorfällen müssen vor Inbetriebnahme festgelegt werden.

Wir empfehlen, sowohl die App als auch die für den Betrieb erforderlichen Backend-Dienste vor der Inbetriebnahme nach vorher festgelegten Kriterien zu prüfen.[10]

Diese können sowohl die Sicherheit der App und der Backend-Dienste als auch funktionale Aspekte umfassen. So sollte darauf geprüft werden, ob die eingesetzten Backend-Dienste gegen unbefugte Zugriffe (z.B. über Test- oder Wartungszugänge) geschützt sind. Ebenso sollte darauf geachtet werden, dass keine unnötigen Protokoll- oder Diagnosedaten generiert werden, über die schutzwürdige Daten oder Informationen gegenüber Dritten offengelegt werden können. Weiterhin sollte geprüft werden, ob die Information über die Verarbeitung von Daten und die ggf. erforderliche Einwilligungserklärung rechtskonform ausgestaltet ist.

6. Laufende Evaluierung

Nach der Inbetriebnahme einer App wird es auf Grund von Fehlerbehebungen oder Änderungen und Anpassungen der Funktionalität erforderlich sein, regelmäßig die bei der Konzeption und Implementierung getroffenen technischen und organisatorischen Maßnahmen zu überprüfen. Hierzu sollten regelmäßige Prüfungen und Sicherheits-Audits der App und der verwendeten Backend-Dienste durch unabhängige Stellen durchgeführt werden. Wir empfehlen insbesondere, die Geeignetheit der getroffenen technisch-organisatorischen Maßnahmen im Rahmen eines kontinuierlichen Verbesserungsprozesses mindestens einmal jährlich zu überprüfen.

Die dargestellten Anforderungen dieses Rundschreibens können als grundlegende Orientierungshilfe für einen rechtskonformen Einsatz von Apps in der Sozialversicherung gesehen werden. Wir erheben keinen Anspruch darauf, den komplexen und sich stetig entwickelnden Themenbereich in Vollständigkeit abgebildet zu haben. Das Rundschreiben ist nicht dazu geeignet, die Würdigung des konkret vorliegenden Einzelfalls zu ersetzen.

---

[10] Vgl. hierzu die unter Punkt 3 angeführten Leitfäden und Orientierungshilfen sowie die Bausteine APP.1.4 und OPS.1.1.6 des BSI-Grundschutzkompendiums.

Für Rückfragen und einen fachlichen Austausch zur Ausgestaltung der Rahmenbedingungen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)