Bundesversicherungsamt

Checkliste

„Datenschutzrechtliche Aspekte im Rahmen von Verträgen nach § 140a SGB V“

DATUM: 01. Oktober 2018
REFERAT: 215
AKTENZEICHEN: 215-400-2334/2018

Vorbemerkungen:

Die nachfolgende Checkliste beinhaltet datenschutzrechtliche Fragestellungen, die im Rahmen von Verträgen nach § 140a SGB V regelmäßig aufzuwerfen und zu beantworten sind. Die Checkliste erhebt weder einen Anspruch auf Vollständigkeit noch ersetzt sie die Pflicht der Vertragspartner zur eigenständigen rechtskonformen Vertragsgestaltung.

Wir bitten, die nachfolgenden Fragen sorgfältig zu beantworten und uns die vollständig ausgefüllte Checkliste im Zusammenhang mit jeder Vertragsvorlage (auch: Vertragsanpassungen) unterzeichnet vorzulegen. Ebenfalls bitten wir um Beachtung, dass diese Checkliste immer wieder aktualisiert wird, so dass die jeweils aktuellste Fassung zu verwenden ist. Diese finden Sie auf der Homepage des Bundesversicherungsamtes unter:

www.bundesversicherungsamt.de/aufsicht/datenverarbeitungdatenschutz
www.bundesversicherungsamt.de/aufsicht/krankenversicherung/rundschreiben

1. Allgemeine datenschutzrechtliche Bestätigungen

a. Der Vertrag enthält Regelungen zur Einhaltung der (sozial)datenschutzrechtlichen Bestimmungen:

der EU-DSGVO	☐	ja	☐	nein
des SGB V	☐	ja	☐	nein
des SGB X	☐	ja	☐	nein
des BDSG	☐	ja	☐	nein

b. Die Abrechnung der im Rahmen des Vertrages erbrachten Leistungen erfolgt direkt zwischen Leistungserbringer und Krankenkasse (1. Variante):

☐ ja ☐ nein

oder:

Die Abrechnung erfolgt über den Vertragspartner auf Leistungserbringerseite (z.B. Managementgesellschaft) bzw. eine von diesem beauftragte andere Stelle (2. Variante):

☐ ja ☐ nein

wenn die 2. Variante zutrifft: die Anforderungen des § 295a SGB V wurden beachtet:

☐ ja ☐ nein

2. Bestätigungen im Zusammenhang mit der datenschutzrechtlichen Information des Versicherten

a. Es liegt eine umfassende Versicherteninformation vor, die sämtliche relevanten Informationen zum Datenschutz enthält. Alle Informationen gemäß Art. 13 DSGVO werden dem Versicherten in transparenter Form übermittelt (Art. 12 Abs. 1 DSGVO):

☐ ja ☐ nein

Dies kann z.B. dergestalt umgesetzt werden, dass der Versicherte nicht verteilt über mehrere Formulare informiert wird, sondern die datenschutzrechtlichen Informationen zusammenhängend in einem Formular dargestellt werden.

b. Die Versicherteninformation enthält Angaben zu Name und Kontaktdaten (mindestens: zustellungsfähige Anschrift) des bzw. der Verantwortlichen (Art. 13 Abs. 1 Buchst. a DSGVO):

☐ ja ☐ nein

Die genannten Angaben sind immer auch hinsichtlich der Krankenkasse(n) aufzuführen.

c. Die Versicherteninformation enthält Angaben zu den Kontaktdaten (mindestens: zustellungsfähige Anschrift) des jeweiligen Datenschutzbeauftragten (Art. 13 Abs. 1 Buchst. b DSGVO):

☐ ja ☐ nein

d. Die Zwecke der Verarbeitung sind in der Versicherteninformation konkret und abschließend benannt (Art. 13 Abs. 1 Buchst. c DSGVO):

☐ ja ☐ nein

Hinsichtlich der Krankenkassen lassen sich alle genannten Zwecke in der abschließenden Befugnisnorm des § 284 SGB V wiederfinden:

☐ ja ☐ nein

Bei Beteiligung einer Managementgesellschaft: auch hinsichtlich der Managementgesellschaft – die der Krankenkasse obliegende Aufgaben wahrnimmt (§ 197b SGB V) – lassen sich alle genannten Zwecke in § 284 SGB V wiederfinden:

☐ ja ☐ nein

e. Alle beteiligten Stellen sind in der Versicherteninformation konkret und abschließend benannt (Art. 13 Abs. 1 Buchst. e DSGVO):

☐ ja ☐ nein

Nicht ausreichend sind z.B. Formulierungen wie „Abrechnungsdienstleister“, „wissenschaftliches Institut“ etc.

f. Alle betroffenen personenbezogenen Daten sind in der Versicherteninformation konkret und abschließend benannt, z.B. „Vor- und Nachname“, „erbrachte Leistungen“, „Diagnosen“:

☐ ja ☐ nein

Nicht ausreichend sind z.B. Formulierungen wie „Meine Daten“, „Abrechnungsdaten“, „insbesondere“, „z.B.“

g. Sämtliche einschlägigen Rechtsgrundlagen der Verarbeitung sind in der Versicherteninformation genannt (Art. 13 Abs. 1 Buchst. c DSGVO):

☐ ja ☐ nein

h. Die konkreten Zwecke, konkreten Empfänger und konkreten Daten sind in der Versicherteninformation nicht isoliert voneinander, sondern zusammenhängend dargestellt, so dass der Versicherte die einzelnen Datenflüsse unmissverständlich erkennen und nachvollziehen kann:

☐ ja ☐ nein

Es ist sichergestellt, dass die Krankenkassen keine Befunddaten der Versicherten erhalten:

☐ ja ☐ nein

Bei Beteiligung einer Managementgesellschaft: es ist auch sichergestellt, dass die Managementgesellschaft – die der Krankenkasse obliegende Aufgaben wahrnimmt (§ 197b SGB V) – keine Befunddaten der Versicherten erhält:

☐ ja ☐ nein

Es ist sichergestellt, dass die zum Zwecke der Abrechnung übermittelten Daten nicht über den Umfang gemäß § 295 Abs. 1b i.V.m. Abs. 1 SGB V hinausgehen:

☐ ja ☐ nein

i. Die Versicherteninformation enthält konkrete Angaben zur Dauer der Speicherung personenbezogener Daten (Art. 13 Abs. 2 Buchst. a DSGVO):

☐ ja ☐ nein

Die Vorgaben des Art. 17 DSGVO und der ergänzenden nationalen Vorschriften wurden beachtet:

☐ ja ☐ nein

j. Die Versicherteninformation enthält Angaben zu den bestehenden Rechten des Versicherten (Art. 13 Abs. 2 Buchst. b DSGVO, Kapitel III DSGVO, §§ 32 ff. BDSG n.F., §§ 83 ff. SGB X n.F.):

Recht auf Auskunft	☐ ja	☐ nein
Recht auf Berichtigung	☐ ja	☐ nein
Recht auf Löschung	☐ ja	☐ nein
Recht auf Einschränkung der Verarbeitung	☐ ja	☐ nein
Widerspruchsrecht	☐ ja	☐ nein
Recht auf Datenübertragbarkeit	☐ ja	☐ nein

Kumulativ bestehende Rechte werden für den Versicherten erkennbar als solche dargestellt, z.B. durch die Verwendung der Formulierung „und“ (nicht: „oder“):

☐ ja ☐ nein

k. Die Versicherteninformation beinhaltet das Recht des Versicherten, die datenschutzrechtliche Einwilligung jederzeit widerrufen zu können (Art. 13 Abs. 2 Buchst. c DSGVO, Art. 7 Abs. 3 DSGVO):

☐ ja ☐ nein

Der Versicherte wird in diesem Zusammenhang auch darüber informiert, dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung davon nicht berührt wird (Art. 13 Abs. 2 Buchst. c DSGVO, Art. 7 Abs. 3 DSGVO):

☐ ja ☐ nein

l. Die Versicherteninformation enthält Angaben zum Beschwerderecht des Versicherten bei der nationalen Datenschutzaufsichtsbehörde (Art. 13 Abs. 2 Buchst. d DSGVO), für die bundesunmittelbaren Krankenkassen: bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI):

☐ ja ☐ nein

m. Die Versicherteninformation enthält Angaben dazu, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte (Art. 13 Abs. 2 Buchst. e DSGVO):

☐ ja ☐ nein

Der Versicherte wird in diesem Zusammenhang informiert, dass er nicht zur Bereitstellung seiner personenbezogenen Daten verpflichtet ist, sondern seine freiwillige datenschutzrechtliche Einwilligung Voraussetzung für die Datenverarbeitung ist:

☐ ja ☐ nein

Der Versicherte wird zu den möglichen Folgen bei Nichtbereitstellung informiert, dass ohne die datenschutzrechtliche Einwilligung eine Teilnahme am Vertrag nicht möglich ist:

☐ ja ☐ nein

Ausnahme: Ist eine Datenverarbeitung zu Evaluationszwecken vorgesehen?

☐ ja ☐ nein

Wenn ja:

Der Versicherte wird zu den möglichen Folgen bei Nichtbereitstellung ergänzend und insoweit differenzierend informiert, dass die diesbezügliche datenschutzrechtliche Einwilligung keine Voraussetzung für die Teilnahme am Vertrag, die Teilnahme also unabhängig davon möglich ist:

☐ ja ☐ nein

n. Alle Angaben gemäß Buchst. b. bis m. sind in der Versicherteninformation direkt (d.h. ohne Medienbruch) enthalten:

☐ ja ☐ nein

Gemäß Art. 12 Abs. 1 DSGVO sind dem Versicherten alle Informationen gemäß Art. 13 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln.

3. Bestätigungen im Zusammenhang mit der datenschutzrechtlichen Einwilligungserklärung des Versicherten

a. Die Einwilligungserklärung wird schriftlich abgegeben:

☐ ja ☐ nein

b. Wenn eine Datenverarbeitung zu Evaluationszwecken vorgesehen ist (s.o. Punkt 2. m.): diesbezüglich wird eine gesonderte, fakultative Einwilligungserklärung eingeholt:

☐ ja ☐ nein

c. Die datenschutzrechtliche(n) Einwilligungserklärung(en) wird/werden im räumlichen Zusammenhang mit der datenschutzrechtlichen Versicherteninformation, d.h. direkt im Anschluss daran, abgegeben (1. Variante):

☐ ja ☐ nein

oder:

Die datenschutzrechtliche(n) Einwilligungserklärung(en) werden auf einem separaten Formular (z.B. der Teilnahmeerklärung) eingeholt (2. Variante):

☐ ja ☐ nein

wenn die 2. Variante zutrifft: die Einwilligungserklärung(en) enthalten die Aussage, dass der Versicherte die beigefügte datenschutzrechtliche Versicherteninformation erhalten und zur Kenntnis genommen hat und sich mit den Inhalten einverstanden erklärt:

☐ ja ☐ nein

d. Es werden jeweils gesonderte Unterschriften für die Teilnahmeerklärung und die datenschutzrechtliche(n) Einwilligungserklärung(en) eingeholt (1. Variante):

☐ ja ☐ nein

oder:

Eine Unterschrift betrifft mehrere Sachverhalte (2. Variante):

☐ ja ☐ nein

wenn die 2. Variante zutrifft: das Ersuchen um Einwilligung erfolgt in einer klaren und einfachen Sprache so, dass es von den anderen Sachverhalten klar zu unterscheiden ist (Art. 7 Abs. 2 DSGVO):

☐ ja ☐ nein

e. Die Einwilligungserklärung wird ausdrücklich freiwillig abgegeben:

☐ ja ☐ nein

4. Bestätigung zur Einheitlichkeit und Widerspruchsfreiheit der Vertragsunterlagen

Es wurde geprüft und sichergestellt, dass die gesamten Vertragsunterlagen (Vertragstext + Anlagen) einheitliche Regelungen enthalten, so dass sich keine inhaltlichen Widersprüche ergeben:

☐ ja ☐ nein

5. Zugangs- und Zugriffsschutz bei digitalen Anwendungen & Gesundheitsdaten

Vertragsgegenstand sind (auch) digitale Anwendungen:

☐ ja ☐ nein

Wenn digitale Anwendungen (auch) Vertragsgegenstand sind: Die an die Sicherheitsmaßnahmen und –standards zu stellenden Anforderungen sind von der Qualifizierung der Daten abhängig. Es gilt der Grundsatz, dass mit gesteigerter Sensibilität der Daten auch ein erhöhtes Sicherheitsbedürfnis besteht. So ist, insbesondere wenn Gesundheitsdaten betroffen sind, ein sehr hohes Schutzbedürfnis gegeben (vgl. Rundschreiben des BVA vom 18. April 2016, Az. 116-820-981/2015).

Die Krankenkasse ist Anbieter der digitalen Anwendung:

☐ ja ☐ nein, Anbieter ist _____

Wenn die Krankenkasse Anbieter ist: unter Berücksichtigung des o.g. Rundschreibens erfolgt eine gesonderte Mitteilung an das Bundesversicherungsamt, welche besonderen Maßnahmen ergriffen werden. Diese Mitteilung ist der Checkliste als Anlage beigefügt:

☐ ja ☐ nein

Wenn die Krankenkasse nicht Anbieter ist: es wird dafür Sorge getragen, dass die besonderen Schutzmaßnahmen durch den Anbieter der digitalen Anwendung in eigener Verantwortung beachtet werden:

☐ ja ☐ nein

Die vorstehenden Bestätigungen beziehen sich auf den folgenden Vertrag:

Vertragspartner: _____

_____

Vertragsgegenstand: _____

_____

_____

Vertragsversion: _____

_____

Datum Unterschrift