LAND BRANDENBURG

Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie

Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie | Postfach 60 11 63 | 14411 Potsdam

Landesunmittelbare Krankenkassen
Kassen(zahn)ärztliche Vereinigung
MDK
Prüfungsstellen nach § 106c SGB

Henning-von-Tresckow-Str. 2 - 13
14467 Potsdam

Bearb.: Herr Sonne
Gesch-Z.: PDK
Telefon: +49 331 866-5513
Fax: +49 331 866-5514
Internet: www.masgf.brandenburg.de
werner.sonne@masgf.brandenburg.de

Bus und Tram: Haltestelle Alter Markt/Landtag
Bahn und S-Bahn: Potsdam Hauptbahnhof

Potsdam, 19. Januar 2018

Der Prüfdienst informiert - Informationen zum Outsourcing (§ 80 SGB X-neu)
hier: Änderungen durch die DSGVO

Der Prüfdienst Brandenburg nimmt die Änderungen zum Outsourcing (§ 80 SGB X-neu) aufgrund die DSGVO zum Anlass, seine Auffassung zur künftigen Handhabung von § 80 SGB X-neu darzustellen.

Im Prinzip regelt § 80 SGB X-neu inhaltlich nichts Neues. Die öffentliche Stelle (im Folgenden: Auftraggeber) muss weiterhin die Auftragsverarbeitung vorab der zuständigen Aufsichtsbehörde melden. Der Abs. 1 stellt noch einmal klar, dass hiermit nicht die datenschutzrechtliche Aufsichtsbehörde gemeint ist, sondern die Rechts- oder Fachaufsichtsstelle des Auftraggebers.

Abs. 2 bestimmt, dass der Auftrag nur erteilt werden darf, wenn „die Verarbeitung im Inland, in einem anderen Mitgliedstaat der EU oder in einem gleichgestellten Staat, ….., erfolgt“.

Abs. 3 regelt die Zulässigkeit. Die Erteilung eines Auftrags zur Verarbeitung von Sozialdaten durch nicht-öffentliche Stellen ist danach nur möglich, wenn

1. beim Auftraggeber sonst **Störungen im Betriebsablauf** auftreten können oder
2. die übertragenen Arbeiten **beim Auftragsverarbeiter erheblich kostengünstiger** besorgt werden können.

Im Hinblick auf Inhalt und Ausgestaltung der Verträge zur Auftragsverarbeitung macht § 80 SGB X- neu im Gegensatz zur bisherigen Regelung keine Ausführungen. Da es sich nach Abs. 1 bei Aufträgen nach § 80 SGB X-neu um Aufträge nach Art. 28 DSGVO handelt, sind die dort ge-

nannten Anforderungen an den Vertrag zur Auftragsverarbeitung somit auch auf die Auftragsverarbeitung von Sozialdaten anzuwenden (vgl. dort insbesondere Abs. 3).

Die Prüfverpflichtung aus § 80 SGB X-alt wird durch die Art. 32 und 28 der DSGVO ersetzt. Danach sind die Auftraggeber verpflichtet, die Überwachung der technisch-organisatorischen Maßnahmen durchzuführen und eine Risikobewertung sowie – bei Vorliegen der Voraussetzungen – eine Folgenabschätzung vorzunehmen.

Die Anforderung in § 80 SGB X-alt „der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber verbleiben“, ist ersatzlos entfallen.

Der Gesetzgeber hatte im Rahmen der II. Novellierung des Datenschutzrechts im Jahr 2010 in § 80 SGB X die Anforderung aufgenommen, dass „der Auftraggeber sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“ hat. Eine ausdrückliche regelmäßige Prüfungspflicht enthält die neue Fassung des § 80 SGB X nicht. Aus § 80 Abs. 1 SGB X-neu ergibt sich jedoch, dass es sich bei einem Auftrag nach § 80 SGB X um einen Auftrag im Sinne des Art. 28 DSGVO handelt. Es gelten daher die Prüfpflichten für Aufträge nach Art. 28 DSGVO.

Der Gesetzgeber hat in Art. 28 Abs. 1 DSGVO aufgenommen, dass eine Datenverarbeitung im Auftrag nur dann erfolgen darf, wenn der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Aus Art. 28 Abs. 3 Ziff. h DSGVO ergibt sich, dass „ der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht oder dazu beiträgt“. Dies bedeutet für den Auftraggeber, dass eine Prüfungspflicht bereits Bestandteil des konkreten Vertrags zur Auftragsverarbeitung werden muss. In welchen Abständen diese Prüfungen zu erfolgen haben, ist in der DSGVO nicht ausdrücklich geregelt. Der Turnus kann in den jeweiligen Verträgen variieren, er sollte sich an dem Schutzbedarf der Daten und dem Risiko orientieren. Zu beachten ist jedoch, dass der Auftraggeber gemäß Art. 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern zusammenarbeiten darf, die hinreichende Garantien dafür bieten, „dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der Personen gewährleistet“. Somit

besteht die Verpflichtung bei den Auftragsverarbeitenden, dass diese Garantien nicht nur zu Beginn sondern während der gesamten Dauer des Auftragsverhältnisses vorliegen müssen.

Bei der Beurteilung des angemessenen Schutzniveaus sind nach Art 32 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Um diese Vorgabe zu erfüllen, sind entsprechende Risikoanalysen auch für den Prozess der Auslagerung erforderlich. Es wird empfohlen, diese Risikoanalysen anhand der Verfahrensbeschreibungen durchzuführen. Neu bei den Risikoanalysen ist, dass nicht das Risiko des Sozialversicherungsträgers, sondern der Schutz der Rechte der betroffenen Person zu bewerten ist.

Wenn Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, sollten die Verantwortlichen die Folgen der Verarbeitung im Vorfeld genau analysieren (Art. 35 i.V. m. Erwägungsgrund 84 DSGVO). Insbesondere sollen die Ursache, die Art, die Besonderheit und die Schwere des Risikos evaluiert werden.

Anlässlich der Anpassung des § 80 SGB X an die DSGVO hat der deutsche Gesetzgeber in der Begründung auf die besondere Schutzbedürftigkeit von Sozialdaten bei der Auftragsdatenverarbeitung hingewiesen und ein hohes praktisches Bedürfnis der Datensicherheit und des Datenschutzes aufgezeigt. Auch in der DSGVO (vgl. Art. 35 Abs. 3 Ziff. b, Artikel 9 Abs. 1 und Abs. 2 h DSGVO, Erwägungsgrund 91) wird darauf verweisen, dass bei „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten“ – und hierzu zählen die Sozialdaten – eine Datenschutzfolgeabschätzung unerlässlich ist.

Die Datenschutz-Folgenabschätzung ist vergleichbar mit der Vorabkontrolle gem. § 4d BDSG. Sie wurde in der Regel – auch mangels Aufnahme der Vorgabe in das SGB – von den Sozialversicherungsträgern nicht durchgeführt.

Welche Kriterien bei einer Datenschutz-Folgeabschätzung gem. Art. 35 DSGVO anzulegen sind, kann aus dem von der Datenschutzkonferenz (DSK) herausgegebene Arbeitspapier Nr.5 zur Datenschutzfolgeabschätzung und aus dem „Working Paper“ der Art. 29-Gruppe (unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) entnommen werden

Wurden für die bereits laufenden Verarbeitungsverfahren keine Vorabkontrollen durchgeführt, sollten sukzessive Datenschutz-

Folgeabschätzung vorgenommen werden, um das Risiko etwaiger Persönlichkeitsrechtsverletzungen zu vermeiden. Wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind, ist die Folgenabschätzung unverzüglich vorzunehmen (Art. 35 Abs. 1 DSGVO.

In Art. 42 DSGVO ist die Einführung von datenschutzspezifischen Zertifizierungen geregelt. Das Zertifikat soll bescheinigen, dass datenschutzrechtliche Anforderungen im Unternehmen eingehalten werden. Gleichzeitig stellt Art. 42 Abs. 4 aber klar, dass selbstverständlich trotz der Zertifizierung das Unternehmen die übrigen Anforderungen der DSGVO Bestimmungen einhalten muss. Der Erwägungsgrund 100 DSGVO stellt heraus, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, um den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu ermöglichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) berichten in ihrem Kurzpapier Nr. 9 vom 15.08.2017 zur Zertifizierung nach Art. 42 DSGVO:
Art. 42 Abs. 4 hebt hervor, dass eine erfolgreiche Zertifizierung eine Organisation (unabhängig davon, ob Verantwortlicher oder Auftragsverarbeiter) nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. ***Ebenso verdeutlicht Art. 42 Abs. 4, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt bleiben****. Ein nach DS-GVO genehmigtes Zertifizierungsverfahren kann jedoch bei aufsichtsrechtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.*
Die Aufsichtsbehörden haben in ihren Kontrollen zwar festgestellt, dass Organisationen oft verschiedenste Zertifikate vorweisen konnten – jedoch war häufig unklar – inwieweit die gesetzlichen Anforderungen an den Datenschutz ausreichend berücksichtigt wurden. Manche bestehende Zertifizierungsverfahren, wie beispielsweise das Informationssicherheitsmanagement nach ISO 27001, decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung.

Das BayLDA hat in seinen aufsichtsrechtlichen Kontrollen nach § 38 BDSG aufgenommen, dass Unternehmen oft verschiedenste Zertifikate vorweisen konnten – jedoch genügten diese bislang in keinem einzigen Fall – um die Fragen aus dem Prüfumfang des BayLDA ausreichend zu beantworten. Meist handelte es sich um Zertifizierungsverfahren, die nur am Rande mit Datenschutz zu tun hatten, statt diesen in den Fokus zu rücken. Zudem war größtenteils nicht transparent, was im Zertifizierungsverfahren tatsächlich geprüft wurde (aus EU-Datenschutz-Grundverordnung (DS-GVO) – Das BayLDA auf dem Weg zur Umsetzung der Verordnung vom 22.06.2016).

Eine Zertifizierung kann damit nach Art. 35 Abs. 3 DSGVO als ein Nachweis herangezogen werden, dass bestimmte Anforderungen des DSGVO eingehalten werden. Damit wird die Kontrolle (z.B. bei einem Einsatz von Dienstleistern) erleichtert. **Die eigenständigen Prüfungen (in der Regel vor Ort) können dadurch nicht ersetzt werden**.

Im Zusammenhang mit dem Outsourcing spielt auch das „Cloud-Computing“ oft eine große Rolle. Vereinfacht gesagt bedeutet „Cloud Computing“, dass Anwendungen, die bislang auf eigenen Computern bereitgestellt wurden, jetzt ausgelagert auf einer externen Infrastruktur betrieben werden. Die Daten und Informationen finden nicht länger innerhalb der eigenen Infrastruktur ihren Speicherplatz, sie werden auf einem anonymen Server mit unbekanntem Standort vorgehalten.

Bei den Cloud Angeboten gibt es allerdings auch Unterschiede. So ist z.B. zwischen einer Public Cloud und einer Private Cloud zu differenzieren.

Durch die beim Public Cloud genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte, die gegebenenfalls im In- und Ausland sind, zu verteilen. Die Steuerung der in Anspruch genommenen Cloud-Dienste erfolgt in der Regel mittels einer Webschnittstelle durch den Cloud-Nutzer selbst. So kann der Nutzer automatisiert die genutzten Dienste auf seine Bedürfnisse zuschneiden. Anbieter von Public Clouds sind u.a. die großen globalen IT-Unternehmen wie Amazon, Google, Hewlett-Packard, IBM oder Microsoft. Diese verarbeiten die Daten auf weltweit verteilten Servern bzw. Serverfarmen, die einem Anbieter oder auch unterschiedlichen Anbietern gehören.

Von einer Private Cloud spricht man, wenn sowohl die Services als auch die Infrastruktur einer Institution unterstehen und von ihr exklusiv genutzt werden, d. h. Leistungen nur für bestimmte (öffentlich rechtliche) Nutzer angeboten werden.

Es wird dazu kommen, dass immer mehr Dienstleister den Sozialversicherungsträgern Verträge anbieten werden, die die Datenspeicherung in einer Euro-Cloud beinhalten. Den vielfältigen Vorteilen, die Cloud Anwendungen bieten, stehen erhebliche Risiken gegenüber. Bei der Auswahl eines Dienstleisters ist daher, insbesondere bei der Verarbeitung von Sozialdaten (besondere Arten personenbezogener Daten nach Art. 9 DSGVO), Vorsicht geboten. Die DSGVO (Art. 28, 32 und 35) fordert in diesem Zusammenhang umfängliche Risikobewertungen und eine Folgenabschätzung. Auch müssen die technischen und organisatorischen Maßnahmen (Art. 32 DSGVO i.V. mit § 64 BDSG) vom Dienstleister erfüllt werden. Die nach Art. 28 Abs. 3 DSGVO geforderten Sicherheitsmaßnahmen sind vom Auftragsverarbeiter umzusetzen. Die Einhaltung ist nachhaltig zu prüfen.

Aus unserer Sicht sind strategische Abhängigkeiten zu einem Dienstleister unbedingt zu vermeiden.

Der Auftraggeber hat die Datenverarbeitung im Auftrag gem. § 80 SGB X-neu der Aufsicht anzuzeigen. Der Anzeige ist eine Sicherheitskonzeption (Art. 32 DSGVO und Erwägungsgrund 83) sowie eine Wirtschaftlichkeitsanalyse (§ 69 Abs. 2 SGB IV) beizufügen. Bei der Sicherheitskonzeption sind die Anforderungen aus „Der Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises Version 2.0 Stand 09.10.2014“ zu beachten.

Bei der Public Cloud wissen die Auftraggeber nicht, an welchem Standort sich die Daten befinden, ad-hoc Prüfungen vor Ort sind daher nicht möglich. Dies schließt aus unserer Sicht die Möglichkeit eine Auftragsdatenverarbeitung aus. Die Private Cloud wäre dagegen – nur bei Erfüllung der weiteren Auflagen – für die Auslagerung von Sozialdaten geeignet.

Insoweit stellt sich für die Institutionen der aktuelle Handlungsbedarf wie folgt dar:
Zur Umsetzung der neuen Anforderungen der DSGVO hat der Auftraggeber mit dem Dienstleister die folgenden Änderungen abzustimmen und ggfs. auch die Verträge anzupassen:

- Umsetzung der erweiterten sicherheitstechnischen und organisatorischen Anforderungen der DSGVO
- vorhandener Regelungen zur Vertraulichkeit oder gesetzlichen Verschwiegenheit
- Bestimmungen bzgl. Unterauftragsverhältnissen
- Informationspflichten
- Hinweispflicht seitens des Auftragsverarbeiters bei rechtswidrigen Weisungen durch den Auftraggeber sowie Übermittlung in ein Drittland
- Dokumentationspflichten des Auftragsverarbeiters
- Dokumentationen des Verzeichnisses von Verarbeitungstätigkeiten
- Unterstützungspflichten des Auftragsverarbeiters
- Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber/ Verantwortlichen bei

    - der Zusammenarbeit mit den Aufsichtsbehörden
    - der Meldung von Datenpannen
    - der Datenschutz-Folgenabschätzung
    - Prüfungen durch den Verantwortlichen oder dessen Beauftragten.

Fazit:

Gemäß Artikel 28 Absatz 1 DSGVO arbeitet der Verantwortliche nur mit Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der Personen gewährleistet. Dies beinhaltet implizit die Verpflichtung, dass diese Garantien nicht nur zu Beginn des Auftragsverhältnisses vorliegen müssen, sondern darüber hinaus während des gesamten Zeitraumes fortgelten.
Wie bisher muss der Auftraggeber vor Beginn der Auftragsverarbeitung und sodann regelmäßig seiner Prüfverpflichtung nachkommen. Aus Revisionsgesichtspunkten ist eine „Vor Ort" Prüfung unerlässlich, da ansonsten der „Ist Zustand" bei dem Dienstleister nicht beurteilt werden kann. Eine Prüfung gegen Dokumente hat den Nachteil, dass nur das „Soll" betrachtet wird.

Bei der Anzeige einer neuen Auftragsdatenverarbeitung nach § 80 SGB X-neu ist insbesondere der Nachweis, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt nebst Risikobewertung einschl. der Folgenabschätzung der zuständigen Aufsicht vorzulegen.

Eine Zertifizierung nach § 42 DSGVO kann als Nachweis herangezogen werden, dass bestimmte Anforderungen des DSGVO eingehalten werden. Damit wird die Einschätzung, „der Dienstleister bietet hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der Personen gewährleistet ist" erleichtert. Die eigenständigen Kontrollen werden im Hinblick auf den besonderen Schutz der Sozialdaten nicht ersetzt. Insoweit spricht der Gesetzgeber in Art 32 DSGVO auch nur davon, dass das Zertifikat als „ein Faktor" herangezogen werden kann, um die Erfüllung der genannten Anforderungen nachzuweisen.

Ein Cloud Computing wird – auch bei Vorliegen der weiteren Anforderungen – rechtlich für nicht zulässig gehalten, wenn der Auftraggeber oder die Aufsichtsbehörden nicht in der Lage sind, mit angemessenem Aufwand die Einhaltung der Vorschriften der DSGVO zu überwachen oder diese Prüfung wegen des nicht bekannten Standortes der Daten - ausgeschlossen ist.

Diese Ausführungen werden auch die Grundlage für unsere künftigen Prüfungen bilden. Sollten Sie Fragen zu diesem Bereich haben, können Sie sich gern an Frau Sonne (Mailadresse: christina.sonne@masgf.brandenburg.de) wenden.

Freundliche Grüße

Werner Sonne