ineges Institut für Europäische Gesundheitspolitik und Sozialrecht

Gesundheitsversorgung in Zeiten der Datenschutz-Grundverordnung (DSGVO)–
Wissenschaftliche Tagung am 18.09.2018 an der Goethe-Universität Frankfurt am Main

Auftrags~~daten~~verarbeitung in der Cloud - Tücken im neuen SGB X und der DSGVO?

Dr. Thomas Lapp, Rechtsanwalt und Mediator, Fachanwalt für Informationstechnologierecht, Datenschutzbeauftragter

1. § 80 SGB X ist auf die DS-GVO abgestimmt worden und statt des Anforderungskatalogs von Abs. 2 SGB X verweist § 80 Abs. 1 S. 1 DS-GVO jetzt auf Art. 28 DS-GVO. Die alte Fassung entsprach weitgehend der Regelung in § 11 Abs. 2 BDSG a.F. Diese Regelungen setzten weitgehend europarechtlichen Vorgaben aus Art. 17 EG-DSRL um. Nach wie vor werden Rechte und Pflichten der Vertragsparteien in wesentlichen Punkten durch die Norm vorgegeben. Dabei wird aber kein neuer Vertragstyp geschaffen, wie es beispielsweise die Schöpfer des BGB getan hätten. Vielmehr wird den Vertragsparteien vorgegeben, welche Regelungen Vertragsgegenstand sein müssen. Spielraum bleibt insbesondere für individuelle sprachliche Formulierungen.
2. Anders als in § 43e BRAO für die Nutzung der Cloud durch Rechtsanwälte werden keine eigenen Anforderungen an die Vereinbarung aufgestellt, sondern auf Art. 28 DS-GVO verwiesen.
3. Vertragspartner müssen Verpflichtungen festlegen, die Ihnen bereits kraft Gesetzes obliegen. Doppelung der Technik soll die Bindung an diese Anforderung verstärken, führt letztlich nur zu umfangreicheren Verträgen.
4. Anwendungsbereich der Auftragsverarbeitung hat sich nicht verändert. Neben klassischem Outsourcing ist auch Cloud Computing umfasst. Funktionsübertragung ist nicht mehr ausgeschlossen.
5. Verträge können als eigenständige Verträge zu Auftragsverarbeitung mit Anlage zu technischen und organisatorischen Maßnahmen geschlossen werden. Die Regelungen können aber auch in den Hauptvertrag integriert werden. Die nach Art. 28 Abs. 3 S. 1 DS-GVO aufzunehmenden Angaben müssen in der Regel vom Auftraggeber unter Mitwirkung des Auftragnehmers, die technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO vom Auftragnehmer in Absprache mit dem Auftraggeber formuliert werden, während Art. 28 Abs. 3 S. 2 a-h) DS-GVO reine Wiederholung des Gesetzestextes vorschreibt.
6. § 80 SGB X beruht auf der Öffnungsklausel Art. 9 Abs. 2 b) DS-GVO, wiederholt in § 22 Abs. 1 BDSG mit Beispielen in § 22 Abs. 2 BDSG. Die Anforderung, den Datenbestand überwiegend beim Auftraggeber oder einem öffentlichen Auftragnehmer zu verarbeiten ist als nicht mehr zeitgemäß entfallen. Dient es den Grundrechten und Interessen der betroffenen Personen, AVV nur zur Abwendung von Störungen im Betriebsablauf oder zu Realisierung von Kostenvorteilen zu gestatten? Ist diese Anforderung von der Öffnungsklausel gedeckt, die geeignete Garantien für die Grundrechte und die Interessen der betroffenen Personen fordert? Der Verweis auf Art. 28 und indirekt Art. 32 DS-GVO, sowie die Mitteilungspflichten können solche Garantien darstellen.
7. § 80 Abs. 1 SGB X verpflichtet die verantwortliche Stelle, der Aufsichtsbehörde die beabsichtigte Auftragsverarbeitung anzuzeigen und dabei eine Reihe von Angaben zu machen. Die erforderlichen Angaben entsprechend teilweise dem vorgeschriebenen Regelungsinhalt Art. 28 DS-GVO. Abweichend davon sind nicht Art und Zweck der Verarbeitung, sondern die mit der Auftragsverarbeitung zu erfüllende Aufgabe darzustellen. Es könnte also die AVV mit ergänzender Information zu dieser Aufgabe vorgelegt werden. Fraglich ist, ob neue Subunternehmer mitzuteilen sind. Öffentliche Auftragnehmer müssen die AVV ihrer Rechts- oder Fachaufsichtsbehörde schriftlich oder elektronisch anzeigen, dabei aber keine bestimmten Angaben machen oder Informationen liefern.

8. § 203 Abs. 3 S. 2 StGB stellt Outsourcing und Cloud Computing in die unternehmerische Entscheidung des jeweiligen Auftraggebers . Erforderlichkeitsprüfung bezieht sich ausschließlich auf die Offenbarung der fremden Geheimnisse.
9. Landesrechtliche Regelungen, wie etwa § 12 HKHG (Hessisches Krankenhausgesetz 2011), weichen teilweise ab und legen strengere Anforderungen fest. AVV stellt aber keine Übermittlung personenbezogener Daten dar.