28.01.2015

Gemeinsame Presseerklärung von
BvD, bvitg, GMDS und GDD

# Verbandsübergreifendes Muster zur Auftragsdatenverarbeitung für das Gesundheitswesen

**Eine verbandsübergreifende Arbeitsgruppe bestehend aus Vertretern des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD, „Arbeitskreis Medizin"), des Bundesverbandes Gesundheits-IT e.V. (bvitg), der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS, Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen") und der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD, Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen") hat ein kommentiertes Muster eines Auftragsdatenverarbeitungsvertrags erarbeitet, die auf die besonderen Belange des Gesundheitswesens eingeht und den Datenschutz bei der Einbindung von Dienstleistern im Gesundheitsbereich sicherstellen soll.**

Der Zugriff auf sensible Patientendaten durch externe Dienstleister unterliegt den Datenschutzgesetzen und muss vertraglich geregelt werden. Die Ergebnisse der Arbeitsgruppe umfassen neben dem so genannten „ADV-Vertrag" auch ein Beispiel zur Anwendung des Musters bei einer Fernwartung sowie jeweils einen Vorschlag zur Vorbereitung einer Prüfung durch den Auftraggeber und einer Selbstauskunft des Auftragnehmers zur Beurteilung seiner Eignung.

Die von der Arbeitsgruppe erarbeiteten Dokumente bieten Krankenhäusern, Arztpraxen und IT-Herstellern eine Hilfestellung, um das Thema Auftragsdatenverarbeitung im Gesundheitswesen so weit wie möglich praxisgerecht für beide Seiten vertraglich umzusetzen.

Die beteiligten Vertreter erklärten, dass zum ersten Mal in Deutschland eine solche Hersteller und Kunden übergreifende Lösung für den Datenschutz im Gesundheitswesen erarbeitet wurde und betonten die produktive Zusammenarbeit aller beteiligten Verbände.

Die Verbände weisen darauf hin, dass allein mit dieser Mustervereinbarung die Anforderungen der ärztlichen Schweigepflicht bei Einbindung von Dienstleistern noch nicht gelöst werden können. Stand heute kann auch mit einer datenschutzrechtlich einwandfreien und gesetzeskonform geregelten Auftragsdatenverarbeitung allein keine Offenbarungsbefugnis gemäß § 203 StGB abgeleitet werden. Im Interesse aller Beteiligten muss durch den Gesetzgeber hier eine ausgewogene Lösung gefunden werden, mit der Dienstleister rechtssicher eingebunden und zugleich das Vertrauen in die verschwiegene Ausübung des ärztlichen Berufes gewährleistet werden.

Alle Materialien sind auf den Internetseiten der Verbände verfügbar:

- BvD: https://www.bvdnet.de/ak-medizin.html

- bvitg: http://www.bvitg.de
- GMDS: http://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen
- GDD: http://gddak.eh-cc.de/materialien_und_links/

Zu den Verbänden:

- BvD: Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) mit Sitz in Berlin vertritt die Interessen von über 800 betrieblichen und behördlichen Datenschutzbeauftragten.
- bvitg: Der bvitg e.V. vertritt in Deutschland die führenden IT-Anbieter im Gesundheitswesen und repräsentiert mit seinen Mitgliedern 90 Prozent des stationären, des ambulanten sowie des zahnmedizinischen IT-Marktes. Über 70 Prozent der Unternehmen sind international tätig.
- GMDS: Die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS) konstituierte sich 1955 und ist damit die älteste unabhängige wissenschaftliche medizinische Fachgesellschaft in Europa auf dem Gebiet der Medizinischen Dokumentation, Informatik und Statistik. Die GMDS hat das Ziel, die Medizinische Informatik einschließlich der Medizinischen Dokumentation, die Medizinische Biometrie und die Epidemiologie in Theorie und Anwendung, in Forschung und Lehre zu fördern. Die GMDS hat ca. 2000 Mitglieder und etwa 50 Arbeits- und Projektgruppen.
- GDD: Die Gesellschaft für Datenschutz und Datensicherheit e.V. mit über 2.600 Mitgliedern und Sitz in Bonn tritt für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz sowie Grundsätze der Selbstkontrolle und Selbstregulierung ein.

# Gemeinsame Erläuterung der Arbeitsgruppe zu den Dokumenten für Auftragsdatenverarbeitung im Gesundheitswesen

„Noch ein Muster für einen ADV-Vertrag? Es gibt doch schon eine Vorlage von…“ Stimmt, es gibt eine Vielzahl von ADV-Vorlagen der verschiedensten Organisationen bzw. Verbänden, welche die Erstellung eines ADV-Vertrages erleichtern. Nur geht leider keine der vorhandenen Vorlagen auf die Besonderheiten ein, die in einer Arztpraxis oder im Krankenhaus gebraucht werden, von der medizinischen Forschung ganz zu schweigen.

Auf die Anforderungen zur integrierten Patientenversorgung von spezialisierten Krankenhäusern und ambulanter Versorgung verbunden mit digitalem Datenaustausch zwischen den Behandlern antworteten sowohl die IT- als auch die Geräte-Hersteller, indem sie die eingesetzten Systeme miteinander vernetzten und hochkomplexe Anwendungen bereit stellten. Weder Krankenhäuser noch Arztpraxen sind heute in der Lage, diese Systeme ohne die Unterstützung durch den jeweiligen Hersteller zu betreiben. Folglich müssen die Hersteller bei der Pflege und Wartung der Systeme das Krankenhaus oder die Arztpraxis unterstützen und mitunter dazu sogar Einblick in Patientendaten bekommen.

Wartung von Systemen gilt als klassischer Fall der sog. Auftragsdatenverarbeitung (ADV), einer „privilegierten“ Form der Funktionsübertragung, für welche der Gesetzgeber vertragsrechtliche Anforderungen (§ 11 BDSG, § 80 SGB X, landesrechtliche Bestimmungen) formuliert. Von den Anforderungen, die der Gesetzgeber an eine ADV stellt, seien exemplarisch die sorgfältige Auswahl des Auftragnehmers sowie ein schriftlicher Vertrag genannt.

Gerade an diesen Vertrag werden im Gesundheitswesen besondere Anforderungen gestellt. Nicht nur das BDSG, sondern aufgrund der Trägerschaft auch länderspezifische oder kirchliche Datenschutzbestimmungen gilt es zu berücksichtigen. Zu den erwähnten, darüber hinausgehenden Besonderheiten gehören u. a.

- Sozialdaten,
- Umgang mit §203 StGB sowie dem Beschlagnahmeschutz,
- Umgang mit Datenverarbeitung außerhalb EU/EWR, d.h. auch Umgang mit EU-Standardvertragsklausen,
- Regelung bzgl. Umgang mit Zurückbehaltungsrecht i.S.v. § 273 BGB,
- Schadensersatz- und Haftungsfragen,
- Regelung der Informationspflichten,
- Umgang mit Zweckänderung durch den Auftragnehmer, z.B. Weitergabe der Daten nach Pseudonymisierung/Anonymisierung,
- … (die Liste könnte noch fortgeführt werden).

Eine Arbeitsgruppe bestehend aus Vertretern von

- Berufsverband der Datenschutzbeauftragten Deutschlands e. V., BvD (Arbeitskreis „Medizin“)
- Bundesverband Gesundheits-IT e. V., bvitg
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V., GMDS (Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“)
- Gesellschaft für Datenschutz und Datensicherheit e. V., GDD (Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“)

hat einen kommentierten Muster-ADV-Vertrag entworfen, der auf diese besonderen Belange des Gesundheitswesens eingeht, andererseits auch Praxishilfen für den Umgang mit dem Thema erstellt.

Die Ergebnisse der Arbeitsgruppe liegen nunmehr vor:

1. Ein ADV-Vertrag für das Gesundheitswesen, mit den drei Teilen
   - Einführung, Allgemeines,
   - dem eigentlichen Vertragsentwurf sowie der jeweiligen Kommentierung,
   - und drei Anhängen,
2. ein Beispiel zur Anwendung des Muster-ADV-Vertrages (als Beispiel wurde die Fernwartung gewählt),
3. Vorschläge
   a) zur Prüfung des Auftraggebers, in wieweit er organisatorisch selbst für die Vergabe einer Auftragsdatenverarbeitung vorbereitet ist
   b) zur Selbstauskunft des Auftragnehmers zur Beurteilung der Eignung des Auftragnehmers durch den Auftraggeber entsprechend den Anforderungen gemäß § 11 Abs. 2 BDSG anhand von Excel-Tabellen.
4. Eine Kommentierung zur Beurteilung der Anwendbarkeit der Auftragsdatenverarbeitung aus Sicht der Regelungen entsprechend dem aktuellen Stand der Ausarbeitung zu der geplanten europäischen Datenschutz-Grundverordnung.

Unklar ist derzeit, inwieweit externe Dienstleister zum Kreis der Gehilfen im Sinne des § 203 StGB gezählt werden dürfen. Stand heute kann auch mit den Regelungen der Auftragsdatenverarbeitung die Fragestellung bzgl. einer aus der datenschutzrechtlich einwandfreien Auftragsdatenverarbeitung resultierenden Offenbarungsbefugnis gemäß § 203 StGB für ganz Deutschland nicht beantwortet werden. Eine gesetzeskonforme Auftragsdatenverarbeitung ist nach aktuellem Recht nicht ausreichend, um eine rechtswidrige Offenbarung von Daten, die einer berufsrechtlichen Verschwiegenheit unterliegen (vgl. § 203 StGB) auszuschließen. Im Interesse aller Beteiligten muss durch den Gesetzgeber hier eine ausgewogene Lösung gefunden werden, die auch den Vertrauensschutz in die Berufsausübung berücksichtigt.

Der von der Arbeitsgruppe erarbeitete Muster-ADV-Vertrag bietet eine Hilfestellung, um das Thema Auftragsdatenverarbeitung im Gesundheitswesen so weit wie möglich praxisgerecht für Auftragnehmer (IT-Hersteller) und Auftraggeber (Arztpraxen, Krankenhäuser, ...) vertraglich umzusetzen.