7.2 Datenschutzbeauftragter

Inhaltsverzeichnis

8. Haftung
   a) Haftung des internen Datenschutzbeauftragten
   b) Haftung des externen Datenschutzbeauftragten
   c) Strafrechtliche Haftung
9. Veröffentlichung und Mitteilung der Kontaktdaten des Datenschutzbeauftragten
10. Abberufung und Kündigung
11. (Einvernehmliche) Beendigung der Tätigkeit
12. Buß- und Strafgeldvorschriften
13. Gewährleistung des Datenschutzes bei nicht-bestelltem Datenschutzbeauftragten
14. Fundstellen

Jeder Verantwortliche muss unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Datenschutz-Grundverordnung erfolgt (Art. 24 Abs. 1 Satz 1 DSGVO). Somit ist der Verantwortliche für die Einhaltung der datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung, des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz selbst verantwortlich. Er wird dabei vom betrieblichen bzw. behördlichen Datenschutzbeauftragten unterstützt und beraten (Art. 29 Abs. 1 Buchst. a DSGVO).
Die Datenschutzbeauftragten sind die „Datenschutzfachkräfte vor Ort". In diesem Sinne sind sie erste Ansprechpartner bei datenschutzrechtlichen Fragen der Betriebs- bzw. Behördenleitung, der Mitarbeiter und möglicher Kunden. Gemeinsam mit den Datenschutzaufsichtsbehörden sollen sie einen möglichst effektiven Datenschutz sicherstellen. Anderseits sind die Datenschutzbeauftragten keine Außenstelle der Aufsichtsbehörden, sondern selbstständig tätig.

1. Bestellungsvoraussetzungen

a) Regelung in der Datenschutz-Grundverordnung

Gemäß Art. 37 Abs. 1 DSGVO müssen zukünftig in drei Fällen interne Datenschutzbeauftragte bestellt werden (1):

– Öffentliche Stellen müssen, sofern sie personenbezogene Daten verarbeiten (unabhängig von der Art der verarbeiteten Daten), stets einen Datenschutzbeauftragten bestellen. Ausgenommen davon sind lediglich Gerichte im Rahmen der rechtsprechenden Tätigkeit.

8.1.1.1 Musterformblatt für das Verzeichnis von Verarbeitungstätigkeiten im Gesundheitswesen

Das nachfolgende Formular dient der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten in Krankenhäusern, Arztpraxen und Heimen. Die *kursiv* gehaltenen Stellen sind durch eigene Angaben zu ersetzen.

MUSTER

Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO

Bezeichnung der Verarbeitungstätigkeit:

_____

□ Erstmalige Beschreibung
□ Änderung der Beschreibung vom _____

Datum der Erstellung des Verzeichnisses:

_____

1. Name und Kontaktdaten

Name des Verantwortlichen *(Leiter des Krankenhauses, niedergelassener Arzt, Heimleiter):*	
Straße:	
Postleitzahl:	
Ort:	
E-Mail-Adresse:	
Telefonnummer:	
Internetadresse:	

8.2.1.1 Mustervertrag zur Auftragsverarbeitung im Gesundheitswesen

Aufgrund der Sensibilität der Daten im Gesundheitswesen sind besonders hohe Anforderungen an die Gewährleistung des Datenschutzes und der Datensicherheit im Rahmen einer Auftragsverarbeitung zu stellen. Dies muss sich auch im entsprechenden Vertrag widerspiegeln. Nachfolgend wurde ein Mustervertrag für die Verarbeitung personenbezogener Daten im Auftrag im Gesundheitswesen entworfen, der die Vorgaben der Datenschutz-Grundverordnung (DSGVO) berücksichtigt. Er ist an den verschiedenen, besonders gekennzeichneten Stellen noch aufgabenspezifisch anzupassen und muss konkretisiert werden. Dies gilt auch für die Empfehlungen bezüglich der technischen und organisatorischen Sicherungsmaßnahmen.
Die im folgenden Beispiel aufgeführten festgelegten technisch-organisatorischen Datensicherheitsmaßnahmen können statt im Vertrag selbst auch in einer Anlage zum Vertrag festgehalten werden.
Die *kursiv* gehaltenen Wörter bzw. Wortteile dienen entweder als Hinweise und/oder sind durch eigene Angaben zu ersetzen.
Der Mustervertrag erhebt keinen Anspruch auf Vollständigkeit.

MUSTER

Mustervertrag zur Auftragsverarbeitung im Gesundheitswesen

Vereinbarung

zwischen

.....

(Name des Verantwortlichen – z. B. Krankenhaus XY oder niedergelassener Arzt AB)
– nachstehend Auftraggeber genannt –
und .....
(Name des Auftragsverarbeiters)
– nachstehend Auftragnehmer genannt –

§ 1 Begriffserläuterungen

(1) Auftragsverarbeitung
Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, handelt es sich um eine Form der Auftragsverarbeitung im Sinne des Art. 24 DSGVO und des § 62 BDSG.

(2) Verarbeitung
Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO).

(3) Verantwortlicher
Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw. die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden (Art. 4 Nr. 7 DSGVO).

(4) Auftragsverarbeiter
Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).

(5) Weisungen
Weisungen des Verantwortlichen (Auftraggebers) schreiben die vorzunehmenden Handlungen/Aktionen/Unterlassungen etc. eines Auftragsverarbeiters (Auftragnehmers) mehr oder weniger detailliert vor.

§ 2 Gegenstand des Auftrags (Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Art der Daten und Kreis der Betroffenen)

a) Umfang und Art der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

10.2.5 Checkliste bezüglich der Gewährleistung des Datenschutzes und der Datensicherheit in einem Krankenhaus

Die folgende Checkliste fußt auf einer Veröffentlichung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (www.datenschutzzentrum.de/medizin/krankenh/checkliste-patientendatenschutz.pdf). Sie wurde komplett überarbeitet, den aktuellen Gegebenheiten angepasst und soll dazu helfen, die Einhaltung des Datenschutzes und der Datensicherheit in einem Krankenhaus zu überprüfen und zu bewerten. Die Checkliste erhebt keinen Anspruch auf Vollständigkeit.

Frage	Ja	Nein	Anmerkungen
Werden bei der Patientenaufnahme nur diejenigen Daten erhoben, die die Krankenhausverwaltung zur Erbringung von Krankenhausleistungen sowie zur Abrechnung benötigt?	☐	☐	
Werden in der medizinischen Aufnahme nur die Daten erhoben, die zum Zweck der Behandlung erforderlich sind?	☐	☐	
Werden eventuell darüber hinausgehende Angaben im Aufnahmeformular als „freiwillige Angaben“ gekennzeichnet?	☐	☐	
Wird dem Patienten eine Kopie des Behandlungsvertrages ausgehändigt?	☐	☐	

10.4.4 Heim-Archivordnung

Die folgenden Ausführungen beziehen sich auf ein Archiv, in dem ausschließlich die **konventionell** geführten Akten eines Heims aufbewahrt werden. Bei einer elektronischen Archivierung müssen andere bzw. zusätzliche Anforderungen erfüllt werden, auf die an dieser Stelle nicht eingegangen wird.
Die manuellen Akten bestehen aus Aufzeichnungen über die Heimbewohner sowie deren eventuellen Pflege- und Behandlungsunterlagen. Die Archivierung dieser Papiere dient im Wesentlichen der Dokumentation der Heimunterbringung und eventuell erfolgter Behandlungen. Diese Dokumentation steht zur Auskunftserteilung insbesondere gegenüber den Heimbewohnern oder für Beweiszwecke im Fall von rechtlichen Auseinandersetzungen zur Verfügung.

Regelungsbedarf

Ein Heimarchiv kann aus einem Standort bestehen oder auf mehrere verteilt sein. Überall sollten aber die gleichen Sicherheitsbestimmungen gelten. So ist unter anderem zu regeln,

- wer Zugriffsberechtigung auf die Akten hat,
- wie die Revisionsfähigkeit der Zugriffe gewährleistet werden kann,
- wie die Räumlichkeiten gegen ein unbefugtes Betreten und die Akten gegen einen unbefugten Zugriff geschützt werden können,
- dass die Unterlagen vollständig und unverfälscht aufbewahrt werden bzw. nachvollzogen werden kann, wer welche Änderungen vorgenommen hat und
- dass jederzeit nachvollzogen werden kann, wo sich die Unterlagen (außerhalb des Archivs) gerade befinden.

Sicherheitsmaßnahmen

Um diese Vorgaben verwirklichen zu können, müssen im Regelfall folgende Sicherheitsmaßnahmen ergriffen werden:

- Das Archiv ist zur Verhinderung eines unberechtigten Betretens stets verschlossen zu halten. Zugang zum Archiv dürfen nur diejenigen Personen erhalten, die Zugriff auf die Akten zur Erfüllung ihrer Aufgaben benötigen und hierfür ausdrücklich berechtigt sind.
- Die Entnahme von Akten oder einzelnen Unterlagen, ihr dadurch bedingter neuer Aufenthaltsort und die Wiedereinbringung müssen revisionsfähig dokumentiert werden.
- Der Umgang mit den archivierten Akten sollte im Rahmen einer Heim-Archivordnung eindeutig geregelt sein (siehe nachfolgende Muster-Archivordnung).

Eine Heim-Archivordnung sollte den Charakter einer Betriebs- bzw. Dienstanweisung haben und sich auf eine entsprechende Vereinbarung mit der Arbeitnehmervertretung stützen.
Das nachfolgende Muster erhebt keinen Anspruch auf Vollständigkeit und muss den jeweiligen technischen, organisatorischen und räumlichen Gegebenheiten des Heims angepasst werden. Die *kursiv* gehaltenen Texte sind durch eigene Angaben zu ersetzen bzw. zu ergänzen.

MUSTER

Heim-Archivordnung

§ 1 Definitionen, Geltungsbereich, Räumlichkeiten

(1) Als Archivgut werden alle archivwürdigen, zur dauernden Aufbewahrung bestimmten Unterlagen bezeichnet, die
– Heimbewohner betreffen und
– entweder im Heim entstanden oder ihm übereignet worden sind,
unabhängig von ihrer Speicherform (im Original, als Kopie oder digitalisiert – z. B. in Form von Mikrofiches). Nicht erfasst sind die im Heiminformationssystem elektronisch gespeicherte Informationen zu den Heimbewohnern sowie personenbezogene Akten und Unterlagen der Heimverwaltung zum Zwecke der Abrechnung.
(2) Die Akten können auch sensible personenbezogene Aufzeichnungen über die Untersuchung und Behandlung von Heimbewohnern beinhalten.
(3) Diese Archivordnung regelt die Erstellung, den Transport, die Herausgabe, die Aufbewahrung und den Umgang mit Akten von Heimbewohnern sowie die Vernichtung dieser Akten, unabhängig davon, in wessen Verantwortungsbereich sich die Akten befinden.
(4) Das Archiv befindet sich in

_____

bzw. *Die Teilarchive sind in folgenden Räumlichkeiten untergebracht:*

_____

_____

_____

Eine dauerhafte Archivierung von Akten außerhalb dieser Räumlichkeiten ist unzulässig.

§ 2 Verantwortlichkeiten

(1) Verantwortlich für die Einhaltung dieser Archivordnung und der zu Grunde liegenden Rechtsvorschriften sind alle Beschäftigten des Heims, insbesondere alle Personen, die Kontakt zu Kranken- und Pflegeakten und zu den darin enthaltenen Patientengeheimnissen haben. Diese Beschäftigten sind zu einem besonders verantwortlichen und datenschutzgerechten Umgang mit dem Patientengeheimnis verpflichtet.