Rödl & Partner

DATENSCHUTZ-GRUNDVERORDNUNG

Herausforderungen und Umsetzung für Pflegeeinrichtungen

1. **Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB):**
Die Pflicht zu Bestellung eines bDSB wird für Pflegeeinrichtungen in aller Regel zu bejahen sein. Jedoch haben in der Pflegebranche zahlreiche Anbieter bislang darauf verzichtet.

2. **Klärung der anzuwendenden Rechtsgrundlage(n):**
Neben der DSGVO tritt zum gleichen Stichtag das Bundesdatenschutzgesetz (BDSG) neu in Kraft. Daneben bestehen Landesdatenschutzgesetze sowie für separate Gesetze im kirchlichen Bereich. Daher sollte man als Pflegeeinrichtung die Frage klären, welche Rechtsnormen anzuwenden sind.

3. **Dokumentationskonzept:**
Auf Grund der Beweislastumkehr wird es wesentlich wichtiger als in der Vergangenheit, die Einhaltung der datenschutzrechtlichen Vorgaben aktiv und laufend zu dokumentieren. Dafür kommt bei komplexeren Betrieben ein Datenschutzmanagementsystem in Frage, in dem alle Fäden zusammenlaufen. Insbesondere das Konzept, nach dem im Unternehmen nicht mehr benötigte personenbezogene Daten gelöscht werden (Löschkonzept), sollte unbedingt schriftlich festgehalten werden.

4. **Identifikation und Argumentation bezüglich besonders sensibler Daten:**
Das Entstehen sogenannter „besonders sensibler“ Daten im Sinne von Artikel 9 DSGVO ist in einer Pflegeeinrichtung praktisch unvermeidbar, da Gesundheitsdaten automatisch zu diesen Daten zählen. Da für die Verarbeitung dieser Daten ein grundsätzliches Verbot mit Ausnahmen gilt, sollte schriftlich festgehalten werden, inwiefern hier eine solche Ausnahme vorliegt.

5. **Verarbeitungsverzeichnis:**
Ebenfalls zwingend notwendig für die Erfüllung der nunmehr umgekehrten Beweislast ist das Führen eines datenschutzrechtlichen Verarbeitungsverzeichnisses. Anders sind die gesetzlich verankerten Betroffenenrechte (Siehe Teil 2 des Artikels) nicht einzuhalten. Im Regelfall ist hierzu nichts oder weniges schriftlich vorhanden, so dass tatsächlich dringender Handlungsbedarf besteht.

6. **Technische und organisatorische Maßnahmen:**
Die DSGVO verlangt, dass das Unternehmen angemessene technische und organisatorische Maßnahmen trifft, um personenbezogene Daten angemessen zu schützen. In Verbindung mit der Beweislastumkehr bedeutet dies, dass das Unternehmen abwägen muss, mit welchen welche Schutzmaßnahmen ein angemessenes Niveau erreicht wird und dass es diese Maßnahmen umsetzen muss. Abwägung, Entscheidung und Maßnahmenumsetzung müssen aus Nachweisgründen dokumentiert sein

7. **Dokumentiertes Verfahren zur Datenschutz-Folgenabschätzung:**
Ein Verfahren zur Datenverarbeitung kann hohe Risiken für die Rechte und Freiheiten von Betroffenen hohe Risiken im Sinne der DSGVO mit sich bringen. In diesen Fällen muss der Verantwortliche, also der Pflegeanbieter, eine sogenannte Datenschutz-Folgenabschätzung durchführen. Wichtig ist dabei insbesondere, dass die Verfahren, die solche Risiken beinhalten, systematisch identifiziert werden und dass sowohl die eigentliche Risikoidentifikation als auch die darauf aufsetzende Datenschutz-Folgenabschätzung dokumentiert werden. Dies wird in der Regel auch papiergebundene Verfahren betreffen, denn das Schutzinteresse gilt unabhängig von der verwendeten Technik.

8 **Interne Anweisungen:**
Mit der DSGVO tritt für die Unternehmen faktisch eine Beweislastumkehr ein. Das heißt, dass die Pflegeeinrichtung oder der Pflegedienst auf Anforderung der Datenschutzaufsichtsbehörden seinerseits belegen können muss, dass die DSGVO in der Einrichtung tatsächlich umgesetzt wird. Ein wichtiger Baustein in dieser Beweisführung sind konsistente und nachweislich bekanntgemachte interne Richtlinien und Anweisungen, beispielweise eine Datenschutzrichtlinie und eine IT-Benutzerrichtlinie

9 **ADV-Verträge anpassen bzw. vereinbaren:**
Die bisherige Regelung der Auftragsdatenverarbeitung erfährt durch die DSGVO eine inhaltliche Anpassung, die in den bisher getroffenen Vereinbarungen umzusetzen sein wird. Viel wichtiger in der Praxis der Pflege dürfte allerdings der Umstand sein, dass Kooperationsverhältnisse mit anderen juristischen Personen, bei denen personenbezogene Daten hin- und herfließen, von den Verantwortlichen bisher noch nicht als Auftragsdatenverarbeitungsverhältnisse wahrgenommen werden und daher bislang noch gar nicht schriftlich geregelt sind. Achtung: Es existiert kein Konzernprivileg – sobald die Partnereinrichtung eine eigene rechtliche Person ist, sind Vereinbarungen zwingend erforderlich.

10 **Schulungen:**
Im engen Zusammenhang mit den Anweisungen an sich steht die Notwendigkeit, Mitarbeiter zum Datenschutz zu sensibilisieren und entsprechend zu informieren. Beispielsweise wird sich die Informationspflicht des Unternehmens im Falle einer Datenpanne kaum erfüllen lassen, wenn die Mitarbeiter nicht geschult sind, Datenpannen zu erkennen und diese zu melden. Auch eine solche Unterweisung sollte aus Gründen der Beweisführung unbedingt dokumentiert sein.

11 **Datenpannen:**
Definition, Workflows, Dokumentation: Für die Meldung einer Datenpanne an die Aufsichtsbehörde wird eine Frist von (nur) 72 Stunden eingeführt. Für das Auslösen einer Meldepflicht genügt dabei bereits die Gefahr, dass personenbezogene Daten in unbefugte Hände gelangt sein könnten. Sorgfältige Verschlüsselungskonzepte, die konsequent nachgehalten und dokumentiert werden, können beispielsweise die Reputations- und Haftungsrisiken reduzieren helfen.

12 **Umsetzung des Auskunfts- und Löschungsrechtes der Betroffenen:**
Schließlich sollte auch ein Prozess dafür eingerichtet sein, dass ein Betroffener – dies kann ein Bewohner, ein Klient, aber auch ein (ehemaliger) Mitarbeiter sein – Auskunft über die bzgl. seiner Person gespeicherten personenbezogenen Daten verlangt oder deren Löschung verlangt. Probleme bereitet hier in aller Regel die nicht hinreichend strukturierte bzw. dokumentierte Landschaft der Systeme und der nicht-technischen Datenspeicherungen, die an verschiedenen Orten bzgl. ein- und derselben Person existieren.

IHR ANSPRECHPARTNER

Christoph Naucke

Betriebswirt (Berufsakademie), Zertifizierter Compliance Officer, Zertifizierter Datenschutzbeauftragter

T +49 911 9193 3628
christoph.naucke@roedl.com