Datenschutz

Nachbessern ist angesagt

Über fünf Monate gilt jetzt in Deutschland die **Datenschutzgrundverordnung der EU.** Doch ein großer Teil der Firmen hat die Bestimmungen noch nicht vollständig umgesetzt. Gerade Pflegeeinrichtungen arbeiten mit sensiblen, personenbezogenen Daten. Mit Hilfe der folgenden Fragen lässt sich überprüfen, ob in einem Unternehmen noch Handlungsbedarf besteht.

Seit dem 25. Mai diesen Jahres gilt die Datenschutzgrundverordnung (DSGVO) der EU. Doch erst knapp ein Viertel (24 Prozent) der Unternehmen in Deutschland hat sie bislang vollständig umgesetzt. Das ergab eine repräsentative Befragung des **Digitalverbands Bitkom** bei über 500 Unternehmen. Weitere 40 Prozent haben die Regeln „größtenteils" umgesetzt, 30 Prozent immerhin „teilweise". Gerade erst begonnen mit den Anpassungen haben fünf Prozent der Befragten – trotz drohender Bußgelder. Dabei lässt sich mit fünf einfachen Fragen klären, ob das Datenschutzmanagement eines Unternehmens auf dem aktuellen Stand ist.

1. Wer ist dazu verpflichtet?

Die neuen datenschutzrechtlichen Vorgaben gelten für jedes Unternehmen, das Daten automatisiert verarbeitet. Das betrifft zunächst alle Unternehmen mit Kundendatenbanken, Personaldatensystemen oder sonstigen IT-Strukturen – somit auch Pflegeeinrichtungen jeder Art. Die Rechtsform ist dabei unerheblich. Jede Pflegeeinrichtung verarbeitet personenbezogene Daten, etwa für Zwecke der Eigenwerbung, der Pflege von Kooperationen oder Netzwerken, zur Durchführung von (Heim-)Verträgen oder von Beschäftigungsverhältnissen. Häufig betreffen die relevanten Prozesse auch das Veröffentlichen einer Heimzeitung, das Informationsangebot im Internet oder die Weitergabe von Daten an Dienstleister (z. B. Kooperations-Apotheke).

2. Was ist erlaubt, was nicht?

Bei der Datenverarbeitung gilt: Die Verarbeitung ist verboten, wenn sie nicht ausnahmsweise erlaubt ist. Die DSGVO und das Bundesdatenschutzgesetz (BDSG) folgen dem sogenannten Verbot mit Erlaubnisvorbehalt. Es bedarf also stets einer gesetzlichen Rechtsgrundlage oder einer Einwilligung der Betroffenen. In Betracht kommen im Bereich der Pflege insbesondere der Erlaubnistatbestand zum Zweck der Durchführung des Behandlungsvertrages (Art. 6 DSGVO) oder der Erfüllung einer rechtlichen Verpflichtung (Art. 6 DSGVO i. V. m. Fachgesetzen). In allen anderen Fällen ist eine Einwilligung erforderlich. Wenn ein Unternehmen zum Beispiel mit einer Apotheke eine Kooperation hinsichtlich der Lieferung von Medikamenten für Bewohner hat, muss für die Weitergabe der Daten eine Einwilligung der betroffenen Personen eingeholt werden.

Dabei dürfen ohnehin nur Daten erhoben werden, die für die Erfüllung der verschiedenen Verträge zwingend erforderlich sind. So zum Beispiel Daten, die für den Abschluss eines Behandlungsvertrages (ambulanter Dienst) oder eines Heimvertrages benötigt werden. Das sind vor allem die klassischen Stammdaten wie Name, Geburtsdatum, Anschrift, Kranken- und Pflegeversicherung sowie unter Umständen weitere Sozialdaten.

Für die sogenannten besonderen personenbezogenen Daten gelten erhöhte Anforderungen. Bio-

Checkliste Datenschutzgrundverordnung (DSGVO)

	Ja	Nein
Haben Sie Ihre Datenschutzerklärung auf der Homepage angepasst?		
Haben Sie ein Verarbeitungsverzeichnis erstellt?		
Haben Sie einen Datenschutzbeauftragten benannt?		
Haben Sie alle Prozesse dokumentiert?		
Sind Ihre Verträge angepasst?		
Haben Sie die erforderlichen Vorlagen erstellt? • Einwilligungserklärungen • Hinweise zur Datenverarbeitung		
Haben Sie Ihre technischen und organisatorischen Maßnahmen geprüft?		

Quelle: Lüders Rechtsanwälte

graphische Daten (Nationalität, Konfession, ehemalige Arbeitgeber etc.) sind im ersten Schritt aus datenschutzrechtlicher Sicht nicht zwingend erforderlich für die Vertragserfüllung. Ebenfalls nicht erforderlich sein dürfte die Verarbeitung von Daten Dritter (z. B. Angehörige). In all diesen Fällen ist die Verarbeitung nur zulässig mit einer gesonderten Einwilligung.

3. Wie werden die Daten erhoben?

Um den neuen Anforderungen gerecht zu werden, ist es unumgänglich, die internen Abläufe zur Verarbeitung personenbezogener Daten zu überprüfen, um zu erkennen, welche Daten zu welchem Zweck und auf welcher Rechtsgrundlage gespeichert werden (z. B. Einwilligung, Vertragserfüllung, Cloud-Umgebung). Diese Verarbeitungsabläufe sollten Unternehmen möglichst genau dokumentieren. Unabhängig davon, ob ein Unternehmen bereits tätig geworden ist oder die Umsetzung noch nicht vorangetrieben wurde, können folgende Fragen hilfreich sein:

- Besteht bereits ein nach neuem Recht erforderliches Verarbeitungsverzeichnis?
- Wurden bestehende Verträge ausgewertet, insbesondere Verträge zwischen Verantwortlichen und Auftragsverarbeitern?
- Stimmen die allgemeinen Rahmenbedingungen?
- Welche Maßnahmen zum Schutz personenbezogener Daten sind vorhanden?
- Wurde ein Datenschutzbeauftragter benannt?

Wichtig ist in diesem Zusammenhang, dass auch die Führungsebene an solchen Überprüfungen beteiligt ist und regelmäßig in die Prozesse zur Datenverarbeitung eingebunden wird. Bei einem etwaigen Verstoß gegen Vorgaben des Datenschutzrechts sind nämlich die Unternehmen in der Pflicht, zu beweisen, dass sie alles richtig gemacht haben – dieser Nachweis kann in der Praxis mitunter schwierig werden.

4. Wer wird wie informiert?

Was bisher galt, gilt seit Mai 2018 besonders: Auch nach dem neuen Datenschutzrecht sind Betroffene bereits bei der Erhebung personenbezogener Daten zu informieren über

- den Verantwortlichen
- einen etwaigen Datenschutzbeauftragten
- den Zweck der Erhebung und Verarbeitung
- die Rechtsgrundlage bzw. die berechtigten Interessen
- das Löschkonzept
- die Betroffenenrechte
- die Notwendigkeit für die zu erbringende Leistung und eine gegebenenfalls beabsichtigte Zweckänderung der Nutzung bzw. Verarbeitung.

Dass eine Information erfolgt ist und welchen Inhalt diese Information hat, sollte ebenfalls dokumentiert werden. Besondere Anforderungen an die Information und die Einwilligung der Betroffenen werden gestellt, wenn personenbezogene Daten von Kindern oder Gesundheitsdaten verarbeitet werden. Diese Anforderungen sollten Sie bei Abschluss neuer Verträge, gleich welcher Art, berücksichtigen.

5. Braucht jedes Unternehmen einen Datenschutzbeauftragten?

Die Antwort auf diese Frage lautet: „Im Zweifel Ja“. Unternehmen haben einen Datenschutzbeauftragten zu benennen, wenn

- ihre Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Z“Iecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- nach dem neuen BDSG bei einer Mindestanzahl von zehn Beschäftigten, die regelmäßig mit der Verarbeitung personenbezogener Daten betraut sind.

Als Datenschutzbeauftragter für eine Firma kommen sowohl eigene, interne Mitarbeiter in Betracht als auch ein externer Dienstleister, der von dem Unternehmen mit dieser Aufgabe beauftragt wird.

Handlungsempfehlungen

Die Datenschutzgrundverordnung der EU gilt bereits seit Mai diesen Jahres. Halten Sie also die Regeln ein und passen Sie Ihre internen Prozesse an. Für eine Umsetzung ist es noch nicht zu spät!

- Betrachten Sie die DSGVO nicht als Belastung, sondern als Chance, die Datenverarbeitung in Ordnung zu bringen.
- Bestellen Sie einen Datenschutzbeauftragten und weisen Sie die Zuständigkeiten für Prozesse der Datenverarbeitung klar zu. Dies erleichtert die Umsetzung immens.
- Überprüfen Sie Ihre Vertragsgrundlagen und IT-Systeme.
- Seien Sie vorbereitet auf eine Prüfung durch die Datenschützer.
- Weisen Sie nach, dass Sie etwas getan haben.
- Dokumentieren Sie Einwilligung und Co.
- Legen Sie einen Ordner an, welcher Musterdokumente enthält.
- Benennen Sie interne Ansprechpartner und Vertreter.

Gastautorin ist Leena Diestelhorst, Rechtsanwältin und Datenschutzbeauftrage bei Lüders Rechtanwälte, Hannover.

„Die DSGVO gilt für jedes Unternehmen, das Daten automatisiert verarbeitet.“

Leena Diestelhorst,
Rechtsanwältin