B/2 Die Bestandsaufnahme

Wenn Sie als Datenschutzbeauftragter benannt und mit den benötigten Ressourcen ausgestattet wurden, wenn die Aufgaben und Zuständigkeiten geklärt und wenn die Kontaktdaten sowohl der Aufsichtsbehörde gemeldet als auch intern bekanntgemacht und auf der Website veröffentlicht wurden, ist es an der Zeit, sich einen Überblick über die verschiedenen Datenverarbeitungsprozesse zu verschaffen. In der Praxis ist es sinnvoll, dies im Rahmen einer Bestandsaufnahme zu machen.

B/2.1 Planung der Bestandsaufnahme

Im Rahmen einer ersten Bestandsaufnahme ist es empfehlenswert, dass Sie als Datenschutzbeauftragter die datenschutzrelevantesten Abteilungen und Unterabteilungen der Gesundheitseinrichtung z. B. anhand eines Organigramms auswählen und sich diese Abteilungen mit Blick auf die räumlichen Gegebenheiten, die eingesetzten Verfahren und die datenschutzrelevanten Prozesse vor Ort ansehen. Dabei ist es hilfreich

- Interviews mit der zuständigen Leitung der jeweiligen Abteilung und
- punktuell Interviews mit unterschiedlichen Aufgabenträgern innerhalb der Abteilung (z. B. Pflegern, Ärzten etc.) zu führen.

Tipp: Ein Organigramm der Gesundheitseinrichtung ist ein guter Ausgangspunkt zur Planung der Bestandsaufnahme.

Zudem können weitere Bereiche aufgenommen werden, die ggf. in einem Organigramm nicht separat genannt werden, aber gleichwohl von Bedeutung sind (z. B. der Empfang).

Sofern eine Vielzahl von medizinischen Fachabteilungen besteht, etwa bei großen Krankenhäusern, können Datenschutzbeauftragte gerade zu Beginn der Bestandsaufnahme an ihre Grenzen stoßen. In einem ersten Schritt kann in solchen Situationen ein Überblick mit Hilfe eines Interviews mit der Leitung der Gesamtabteilungen (z. B. dem ärztlichen Direktor) und Interviews mit einer Auswahl von repräsentativen Fachabteilungen hergestellt werden.

Ziel der Vor-Ort-Termine sollte dabei sein:

- sich einen Überblick über die datenschutzrelevanten Prozesse in der Abteilung zu verschaffen und etwaigen Optimierungsbedarf zu dokumentieren;
- die eingesetzten Softwareverfahren, mit denen personenbezogene Daten verarbeitet werden, zu identifizieren und zu überprüfen, ob die relevanten Verfahren bereits im Verzeichnis der Verarbeitungstätigkeiten aufgenommen wurden oder noch aufgenommen werden müssen;
- Auftragsverarbeitungsverhältnisse zu identifizieren, in denen die Gesundheitseinrichtung als Auftraggeber oder Auftragnehmer auftritt;
- bestehende datenschutzrelevante Dokumente (Richtlinien, Formulare, Verträge, Einwilligungserklärungen, Fragebögen etc.) zu identifizieren, zu sichten und ggf. zu sammeln, um diese später im Detail bewerten und auf etwaigen Optimierungsbedarf hinweisen zu können.
- Ein weiteres Ziel der Bestandsaufnahme ist es, die konkreten Ansprechpartner der einzelnen Abteilungen kennenzulernen, offene Fragen entgegenzunehmen und ggf. schon durch das Bestandsaufnahmegespräch für datenschutzrechtliche Themen sensibilisieren zu können.

Ein Ansatz, der sich in der Praxis für die Durchführung von Bestandsaufnahmen bewährt hat, sind freie Interviews ohne detaillierte Gesprächsleitfäden oder Checklisten. Die jeweiligen Ansprechpartner sollten gebeten werden, die alltäglichen Standardsituationen, in denen personenbezogene Daten verarbeitet werden, zu erklären. Es ist dabei häufig hilfreich, sich den „Werdegang" einer betroffenen Person bzw. einer Datenverarbeitung chronologisch erklären zu lassen. Dabei können u. a. folgende Fragen relevant werden:

- Wann kommt die Abteilung das erste Mal in Kontakt mit den Daten (eines Bewerbers, Beschäftigten, Patienten, Angehörigen etc.)?
- Woher stammen die Daten?
- Wie wird mit der betroffenen Person bzw. ihren Daten weiter umgegangen und was sind die weiteren Standardprozesse?
- In welchen Verfahren werden die Daten verarbeitet?
- Werden die Daten an andere Abteilungen oder an andere Unternehmen bzw. Behörden übermittelt?
- Was geschieht noch mit den Daten und an welchen Stellen werden Weichen in der Datenverarbeitung gestellt?

- Wann sind die Daten nicht mehr erforderlich und wann werden die Daten gelöscht?

Hauptsächliches Ziel der Bestandsaufnahme ist es, einen Überblick über die relevanten Prozesse, Verfahren und Auftragsverarbeitungen zu erhalten. Dabei muss nicht jeder Prozess im kleinsten Detail erfasst werden. Im Gegenteil bestünde dann die Gefahr, dass die Bestandsaufnahme ihr Ziel nicht erreicht. Einzelne Prozesse, Verfahren oder Auftragsverarbeitungsverhältnisse können später immer noch im Detail untersucht, dokumentiert und bewertet werden. Im Rahmen der ersten Bestandsaufnahme geht es erst einmal darum, die grundlegenden Dinge zu identifizieren.

Tipp: Für eine erste Bestandsaufnahme reicht es häufig aus, pro ausgewählter Fachabteilung einen Vor-Ort-Termin von jeweils ein bis vier Stunden einzuplanen.

B/2.2 Zentrale Punkte verdeutlichen

Vor der Bestandsaufnahme ist es ratsam, sich noch einmal die zentralen Punkte zu verdeutlichen, für deren Überwachung Sie als Datenschutzbeauftragter Sorge zu tragen haben:

- Für alle Verfahren muss ein angemessenes Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DS-GVO vorliegen (vgl. B/3).
- Sofern die Gesundheitseinrichtung Auftragsverarbeitungen für andere Verantwortliche erbringt, muss überwacht werden, ob ein Verzeichnis der Auftragsverarbeitungen nach Art. 30 Abs. 2 DS-GVO vorliegt (vgl. B/4).
- Es muss ein angemessener Prozess etabliert sein, der regelt, wer wann und nach welchen Maßstäben eine Datenschutz-Folgenabschätzung durchführt (vgl. B/5).
- Zudem muss überwacht werden, ob die nach Art. 28 DS-GVO erforderlichen Verträge zur Auftragsverarbeitung geschlossen wurden (vgl. B/6) – unabhängig davon, ob die Gesundheitseinrichtung Auftragsverarbeitungen für andere Verantwortliche erbringt oder selbst externe Dienstleister als Auftragsverarbeiter einsetzt. Sofern die Gesundheitseinrichtung selbst externe Dienstleister als Auftragsverarbeiter einsetzt, muss

überprüft werden, ob dies mit der beruflichen Schweigepflicht vereinbar ist – etwa nach den jeweiligen Krankenhausdatenschutzgesetzen der Länder oder nach § 203 StGB (s. dazu schon oben A/3.4.2).

- Es muss überwacht werden, ob die Gesundheitseinrichtung Prozesse implementiert hat, die die Einhaltung von fristgerechten Melde- und Benachrichtigungspflichten nach Art. 33, 34 DS-GVO bei Datenpannen gewährleisten (vgl. B/7).
- Auch die Prozesse zur Umsetzung von Informationspflichten und Betroffenenrechten müssen überwacht werden (vgl. B/8 und B/9).
- Es ist zudem zu überwachen, ob für Mitarbeiter die erforderlichen Sensibilisierungsmaßnahmen und Schulungen durchgeführt wurden bzw. geplant sind (vgl. B/10 und B/11).

Insgesamt sollte der Datenschutzbeauftragte auch im Rahmen der Bestandsaufnahme einen Überblick dafür bekommen, ob die eingesetzten Verfahren, die Prozesse und die Verarbeitungen datenschutzrechtlich rechtmäßig vorgenommen werden und im Einklang mit den Grundsätzen nach Art. 5 DS-GVO stehen (s. zu diesen A/3).

B/2.3 Ziele der Bestandsaufnahme

Nach der Bestandsaufnahme sollten Sie als Datenschutzbeauftragter im Hinblick auf den IST-Zustand des Datenschutzes in der Gesundheitseinrichtung sprachfähig sein und erkannten Optimierungsbedarf gegenüber dem Verantwortlichen und den entsprechenden Ansprechpartnern z. B. im Rahmen einer Bestandsaufnahmepräsentation kommunizieren. Im Anschluss können Sie dann beratend bei der Umsetzung von Maßnahmen zur Verbesserung des Datenschutzes mitwirken und in Zukunft ein Datenschutzmanagementsystem aufbauen, welches kontinuierliche und sich wiederholende Prozesse vorsieht, um den Stand des Datenschutzes stets zu verbessern bzw. auf einem angemessenen Niveau zu halten.