Dr. Gerald Ganzger

Rechtsanwalt & Managing Partner der Lansky, Ganzger & Partner Rechtsanwälte GmbH mit den Schwerpunkten Prozessvertretung, Medien- und Wettbewerbsrecht. Er ist Lektor für Medienrecht an der FH Wien und Leiter des Arbeitskreises „Compliance im Gesundheitswesen" der Karl Landsteiner Gesellschaft.

Ing. Mag. Amra Bajraktarevic

ist in Wien als Rechtsanwaltsanwärterin mit Spezialisierung auf Zivil-, Kartell- und IT-/IP-Recht tätig und unterstützt seit 2010 das juristische Team der international aktiven Wirtschaftskanzlei LANSKY, GANZGER + Partner. Durch ihre Ausbildung und langjährige Tätigkeit als Netzwerkadministratorin hat sie das technische Knowhow, IT-Projekte kompetent zu begleiten. Der Postgraduate-Lehrgang „Informations- und Medienrecht" rundet ihr Profil ab.

Checkliste zur DSGVO für Gesundheitsbetriebe

Die fortschreitende Digitalisierung und Vernetzung erleichtert die Verarbeitung gesundheitsrelevanter personenbezogener Daten nicht nur, sie geht auch mit zahlreichen Pflichten einher, die durch die Europäische Datenschutz-Grundverordnung („DSGVO") weitere Verschärfungen erfahren.

Da die DSGVO keine Umsetzungsfristen kennt, stehen Gesundheitsunternehmen vor der großen Herausforderung, sich bis zu ihrem Inkrafttreten am 25.05.2018 zu rüsten und rechtzeitig sämtliche erforderlichen technischen sowie organisatorischen Maßnahmen zu setzen.

Die folgende Checkliste enthält die wesentlichen zu ergreifenden Maßnahmen und soll als „10-Punkte-Programm" bei der Umsetzung des DSGVO-Projekts unterstützen, wobei insbesondere im ersten Abschnitt „Erhebung des Status quo" auf die spezifisch im Gesundheitsbereich zu erhebenden Daten aufmerksam gemacht wird.

1. Punkt:
Erhebung des Status quo der Datenverarbeitung

1.1 Zu erheben ist im Wesentlichen wie folgt:

- Welche Daten werden verarbeitet?
- Wie werden diese Daten gesammelt?
- Wie und wie lange werden Daten aufbewahrt?
- Wohin und an wen werden Daten weitergegeben?

1.2 Status quo Datenlandschaft

1.2.1 Welche Patientendaten werden erhoben?

- Personendaten: Name, Geburtsdatum, Anschrift, Sozialversicherungsnummer des Patienten sowie von Angehörigen, Bezugspersonen und Erziehungsberechtigten
- Administrative Daten: Aufnahmedaten, Notfalldaten (Kontaktinformationen im Notfall), Daten des zuweisenden Arztes, Informationen betreffend Blut- und Organspender und Patientenverfügungen, Versicherungsdaten, Daten über spezielle „Wahlleistungen", Verrechnungsdaten
- Medizinische Daten: anamnetische Daten, Diagnosen und Therapien, diagnostische und therapeutische Daten wie Befunde, Laborwerte, Einwilligungserklärungen (Aufklärungs- und Einwilligungsbögen)
- Genetische Daten

1.2.2 Welche Mitarbeiterdaten werden erhoben?

- Allgemeine Personendaten: Persönliche Daten, Familie (Herkunft, Religion), Kinder, Finanzdaten (Konto, Versicherung), Bewerbungsschreiben, Ausbildungsnachweise, Dienstzeugnisse psychologische bzw. Einstellungstests, Einstellungsdaten sowie Daten zum Dienstverhältnis (Dienstanweisungen, überlassene Betriebsmittel, Versetzungen, Verweise, Ermahnungen)
- Krankheitsdaten, Untersuchungen (Hygiene), besondere Gesundheitsdaten (Allergien, Autoimmunerkrankungen, psychiatrische Behandlungen etc)

1.2.3 Welche Daten werden im Zusammenhang mit dem Personalmanagement erhoben?

- Wer ist Betriebsrat?
- Welche Betriebsvereinbarungen gibt es (Policies zu Email- und Internet-(Privat-)Nutzung, Diensthandys, Telefone)
- Welche Überwachungsmaßnahmen (zB Telefonüberwachung) gibt es?
- Personalbeurteilungssysteme (Mitarbeiterfragebögen, -beurteilungen uä)?
- Whistleblowing-Hotlines?
- Welche Daten werden in diesen Zusammenhängen verarbeitet?

1.2.4 Welche Daten werden von Kooperationspartner und Lieferanten erhoben?

- zB Reinigungspersonal und Großküche: welche Daten werden verarbeitet?

1.3 Status quo der Datenerhebung

- Werden während des stationären/ambulanten Aufenthaltes bzw bei einer Wiederaufnahme weitere Daten erhoben?

- Werden über die Lohn- und Gehaltsverrechnung sowie das Dienstverhältnis hinausgehende Mitarbeiterdaten erhoben?
- Was ist die Rechtsgrundlage dieser Datenerhebung (zB schriftliche/mündliche/konkludente Einwilligung des Patienten/Mitarbeiters)?
- Was ist der Zweck der Datenverarbeitung (zB Medizinische Versorgung, Lehre, wissenschaftliche Forschung, Verrechnung von (Wahl-) Leistungen, Archivierung, Statistiken, Qualitätsmanagement; Gehaltsabrechnung, Personalbeurteilung, Dienst- und Einsatzplanung)?
- Wo bzw wie werden diese Daten gespeichert (elektronisch/Papierform/zentral/dezentral/cloud)?
- Wer hat Zugriff auf diese Daten (zB behandelnder Arzt, Fachabteilung, medizinisches Personal, Personalabteilung)?
- An wen werden Daten weiterübermittelt (zB zuweisender Arzt, interne bzw externe Fachabteilungen bzw Fachärzte, Verrechnungsstellen, gesetzliche und private Versicherungsträger, Lohnverrechnung)?
- Wie lange werden diese Daten aufgehoben?
- Werden Daten auf dem aktuellen Stand gehalten (Möglichkeit der Berichtigung vorhanden)?
- Was passiert mit Daten nach Erreichung des Zwecks (zB Anonymisierung/Löschung/längere gesetzliche Aufbewahrungspflicht)?
- Wie erfolgt der Löschungsprozess (manuell/automatisch/Sperre oder physische Löschung)?

1.4 Status quo der Systemlandschaft

1.4.1 Softwaresysteme zur Datenverarbeitung

- Welche Systeme gibt es, in denen Daten verarbeitet werden?
- Welchen Zweck haben diese Systeme (zB Patientendatenverwaltung, Rechnungswesen, Personalverrechnung, Datenübermittlung, Zutrittskontrollsystem, Marketing & PR, etc)?
- Werden die Daten für andere Zwecke bzw in anderen Systemen weiterverarbeitet?
- Ist die Weiterverarbeitung mit dem ursprünglichen Zweck der Datenerhebung vereinbar?
- Werden die Daten an Auftragsverarbeiter (früher Dienstleister) überlassen?
- Werden die Systeme ferngewartet?
- Ist die rechtliche Befugnis zur Datenverarbeitung (zB Gewerbeberechtigung) auch bei den Auftragsverarbeitern vorhanden?
- Besteht eine Rechtsgrundlage für die Datenüberlassung (Vertrag mit Auftragsverarbeiter, zB auch Vertrag mit Drucker-Fernwartungsunternehmen, da hier Daten im Cache gespeichert werden und auslesbar sind)?
- Werden die Daten an Dritte übermittelt bzw veröffentlicht (zB Rettungsdienste, Großküche, uä)?
- Finden Datenübermittlungen im Konzern bzw unter verbundenen Unternehmen bzw in Nicht-EU-Staaten statt?
- Gibt es eine Rechtsgrundlage für die Datenübermittlung/Veröffentlichung (zB Einwilligung des Betroffenen)?

1.4.2 Bauliche Ausgestaltung der IT-Systeme

- Wer hat Zutritt zu Serverräumen, Büros, etc?
- Gibt es Zutrittskontrollen bzw Zutrittskontrollsysteme?
- Ist Zutritt durch nicht-zutrittsberechtigte Dritte möglich?

1.4.3 Technische Ausgestaltung der IT-Systeme

- Wer hat Zugriff (zB VPN-Systeme, Fernwartung durch IT-Dienstleister, offenes bzw gesichertes Patienten-/Mitarbeiter-WLAN, Diensthandys)?
- Gibt es Zugriffskontrollen?
- Gibt es Verschlüsselungssysteme?
- Sind Firewall und allenfalls Data Intrusion Systems implementiert?
- Wird Anti Viren Software regelmäßig aktualisiert?
- Welche Vorkehrungen werden für die Datensicherheit und Integrität der Daten getroffen (Datenwiederherstellungsprozesse, Backups, Archivierung)?

1.4.4 Erhebung Status Quo der Videoüberwachung

- Ist die Videoüberwachung gekennzeichnet?
- Was ist Zweck der Videoüberwachung (besondere Vorkommnisse/besondere Gefährdung)?
- Wie erfolgt die Videoüberwachung (Echtzeit/dauerhaft)?
- In welchen Zeiträumen erfolgt Videoüberwachung (non-Stop, nur Werktags, uä)
- Welche Räumlichkeiten werden videoüberwacht (Außenbereich/Innenbereich, hier insb welche Räume)
- Welche Personen werden gefilmt (Patienten, Besucher, Mitarbeiter, Passanten)?
- Ist die Kameraposition fix oder schwenkbar?
- Werden auch Tondaten erfasst?
- Wo werden Daten gespeichert (analoges/digitales Speichermedium)?
- Wie lange werden Daten gespeichert?

- Werden gespeicherte Daten verschlüsselt?
- Erfolgt eine Auswertung der Videodaten?
- Erfolgt eine elektronische/automatisierte Auswertung der Videodaten?
- Werden biometrische Daten verarbeitet?
- Können gefilmte Personen durch Software unkenntlich gemacht werden?

1.4.5 Erhebung Status Quo der Unternehmensorganisation

- Gibt es definierte Verantwortliche(Datenschutzbeauftragter, Verantwortlicher bei Betroffenenanfragen)?
- Gibt es definierte Abläufe
  - für die Einhaltung der Grundsätze der DSGVO (zB Löschen von Daten nach Zweckerreichung, Akten- bzw Datenträgervernichtung, etc)?
  - für die Erfüllung von Betroffenenrechten?
  - bei Datenlecks und Data Breaches?
  - bei Zusammenarbeit mit Dienstleistern?

1.4.6 Status quo der Verträge mit Auftragsverarbeitern

- Welche Verträge wurden mit Auftragsverarbeitern
- Evaluierung, inwieweit diese Verträge an die neue Rechtslage anzupassen sind (insbesondere Haftungsbestimmungen).
- Evaluierung der bestehenden Versicherungen hinsichtlich Datenschutz und Anpassung an die neue Rechtslage.

2. Punkt:
Einrichtung eines Datenschutz-Compliance-Systems

2.1 Erstellung einer Datenschutzstrategie/Datenschutz-Policy
- Festlegung Ziele, interne Rollen, Verantwortlichkeiten der Datenverarbeitung und Auswertung Risiko für Rechte und Freiheiten der Betroffenen
- Festlegung technische und organisatorische Sicherheitsmaßnahmen in Bezug auf Datenverarbeitung, zB
  - Datenbank- und Speicherkonzepte
  - Zugriffskonzepte
  - Anonymisierungs- und Pseudonymisierungskonzepte
  - Löschkonzepte

2.2 Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten

2.3 Erstellung einer Datenschutz-Folgenabschätzung

2.4 Festlegung der Verantwortlichkeiten für die Verpflichtungen nach der DSGVO, insbesondere für die Gewährleistung der Betroffenenrechte

2.5 Festlegung von Abläufen bei Anfragen/Anträgen von betroffenen Personen

2.6 Festlegung von Notfallstrategien

3. Punkt:
Bestellung eines Datenschutzbeauftragten

3.1 Für Krankenhäuser und Gesundheitsbetriebe in der Regel verpflichtend, aber auch sinnvoll, wenn ein Datenschutzbeauftragter nicht obligatorisch ist.

3.2 Entscheidung, ob interner oder externer Datenschutzbeauftragter

3.3 Bestellung eines Datenschutzbeauftragten („Datenschutzmanager“) auch für Tochtergesellschaften

4. Punkt:
Prüfung der Datenschutzzustimmungserklärungen

4.1 Zeitpunkt der Einwilligung vor Erhebung der Daten?

4.2 Enthält die Erklärung inhaltlich …
- Art der von der Verarbeitung betroffenen Daten
- Zweck der Datenverarbeitung (Sonderfall: wissenschaftliche Forschung)
- der/die Verantwortlichen
- Speicherdauer der Daten
- Widerrufsmöglichkeit

4.3 Formelle Prüfung

- Einwilligungsfähigkeit der betroffenen Person (Einwilligung von Personen unter 14 Jahren)
- Freiwilligkeit (liegt ein Abhängigkeitsverhältnis vor?)
- Klare und einfach verständliche Formulierung
- Nachweisbarkeit

4.4 Werden erteilte Einwilligung protokolliert und sind jederzeit abrufbar?

5. Punkt:
Prüfung der bisher verwendeten Formulare

5.1 Evaluierung bislang verwendete Formulare (zB Aufklärungs- und Einwilligungsbögen, aber auch Zustimmungserklärungen in AGB)

5.2 Evaluierung Formularpolitik in Tochtergesellschaften

5.3 Anpassung der Formulare an die Anforderungen der DSGVO

6. Punkt:
Einrichtung eines Kontrollsystems

6.1 Erweiterung internes Kontrollsystem um Datenschutz

6.2 Festlegung der Verantwortlichkeiten im Zusammenhang mit Kontrolle der Datenschutzstrategien,

Sicherheitssysteme und technischen sowie organisatorischen Maßnahmen

6.3 Festlegung von Kontrollprozessen (wann werden Stichproben gezogen etc)

7. Punkt:

Einrichtung eines Dokumentationssystems

7.1 Entsprechend der Rechenschaftspflicht sind alle Vorgänge zu protokollieren und dokumentieren, insbesondere

- Wahrnehmung Informationspflichten
- Erteilung von Datenschutzzustimmungserklärungen
- Anträge von Betroffenen und deren Erledigung
- Interne Kontrollen
- Personalschulungen

8. Punkt:

Prüfung und Adaptierung der Verträge mit Auftragsverarbeitern

- Evaluierung Verträge mit Auftragsverarbeitern, insbesondere
- DSGVO-Konformität
- Wirksamkeit für gesamte Unternehmensgruppe
- Regressmöglichkeiten
- Versicherungsdeckung bei Verstößen

9. Punkt:

Implementierung Datenschutz durch Technik

- Evaluierung, ob IT-Systeme dem Stand der Technik entsprechen
- Evaluierung Komatibilität Systeme mit Sicherheitsmaßnahmen
- Implementieren von technischen Compliance-Maßnahmen (Privacy by design/default)
- Implementieren von verpflichtenden Sicherheitsmaßnahmen (Art 32 DSGVO)

10.Punkt:

Information und Schulung der Mitarbeiter

- Schulungskonzept für Mitarbeiter, insbesondere auch bei Neueintritt, die dem Aufgabenbereich der Mitarbeiter entsprechen
- Dokumentation der Information
- Protokollierungen Schulungen und Informationen im Personalakt

Diese Checkliste ist nur eine Orientierungshilfe; selbstverständlich wird es notwendig sein, die spezifischen Anforderungen des jeweiligen Gesundheitsbetriebs zu berücksichtigen.