Prüferfahrungen in Kliniken

Dipl.-Inform. Corina Scheiter

Geschäftsstelle des Bayerischen
Landesbeauftragten für den Datenschutz

Agenda

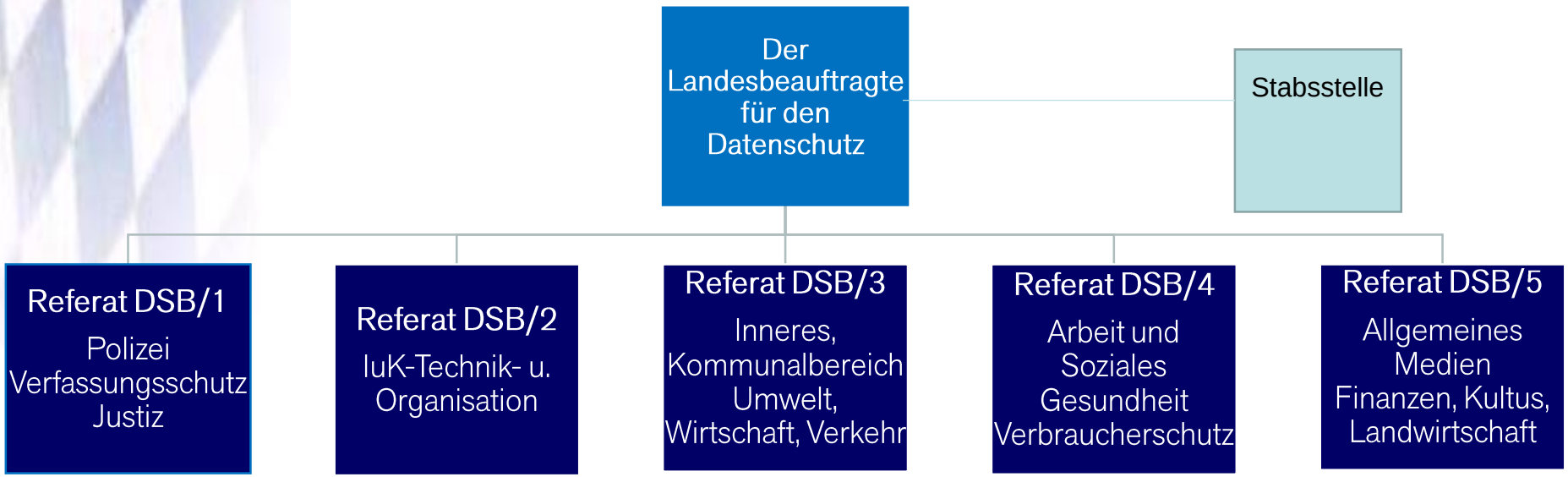
- Vorstellung und Aufgaben BayLfD
- Varianten von Prüfungen
- Bisherige Prüfungen
  - Historie
  - Typische Themen
  - Kriterien für technische Prüfungen
  - Beispiele
- Änderungen durch die DSGVO (insbesondere im technischen Bereich)
- Erste Prüfungen nach DSGVO

Vorstellung BayLfD

- Seit 01.07.2009 Prof. Dr. Thomas Petri
- Datenschutzaufsicht für die öffentlichen Stellen in Bayern, d.h. auch öffentliche Krankenhäuser, Universitätskliniken
- Tätigkeiten
  - Stellungnahmen zu Gesetzentwürfen, Projekten etc.
  - Bearbeitung von Petitionen, Erteilung von Auskünften an Bürger
  - Beratung öffentlicher Stellen
  - Anlass(un)abhängige Prüfungen

Vorstellung BayLfD

DER BAYERISCHE LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ



Prüfungsvarianten

- Wie wir prüfen
  - Anlassbezogen, anlassunabhängig
  - Rechtlich, technisch-organisatorisch, gemeinsam
  - Vor-Ort, schriftliches Verfahren, automatisiert
  - Stichproben, alle Krankenhäuser
  - Allgemein, spezielle Fragestellungen

Historie

Technisch-organisatorische Prüfungen begleiten die technologische Entwicklung

- Big Data, medizinische Forschung, genetische Daten
- Cloud, mobile Geräte, BYOD, Apps
- Intersektorale Vernetzung, eGK, Telemedizin
- Beteiligung von Dienstleistern, AuftragsDV, Fernwartung
- Elektronische Akten
- Vernetze IT-Systeme und medizinische Großgeräte
- Einzelne Computer und medizinische Geräte
- Papiergebundene Verfahren, Mikroverfilmung

Typische Prüfungsthemen

- Nicht datenschutzgerechte Entsorgung
- Patientenakten auf dem Gang
- Verlust von Akten, Vollständigkeit von Akten
- Pfarrerlisten, Pfortenauskunft
- Archivierung (bei externen Dienstleistern)
- Scannen (durch externe Dienstleister)
- Schutz von Computern (Passwortaufbewahrung, Sicherung Laufwerke)
- E-Mail-Versand, Fax
- Sichere Internetanbindung

Typische Prüfungsthemen

- Themen OH KIS
  - Hinzuziehung von Vorbehandlungsdaten
  - Sperren von Patientendaten nach der Entlassung
  - Versand von Arztbriefen an niedergelassene Ärzte
  - Abschaffung von Gruppenkennungen
  - Differenzierte, dynamische Berechtigungskonzepte
  - Datenlöschung im KIS
- Nutzung von Privatgeräten
- Cloud-Lösungen
- Apps, Messenger-Dienste

Typische Prüfungsthemen

- Auswahl und Nutzung von Behandlungsdaten für die Forschung
- Pseudonymisierung
- Umgang mit Biomaterialien
- Multicenter-Studien
- Gesicherte Kommunikationsinfrastruktur mit externen Partnern, Zuweiserportale, Telemedizin
- Internetauftritt, Datenschutzerklärung, Kontakformulare
- Videoüberwachung

Technische Kriterien - bisher

- Art. 7 BayDSG, § 9 BDSG und Anlage
- Umsetzung Datenschutz-Basisanforderungen: Zweckbindung, Erforderlichkeit
- Orientiert an IT-Sicherheitskriterien
  - Vertraulichkeit
  - Authentizität
  - Integrität
  - Verfügbarkeit
  - Revisionsfähigkeit

Technische Kriterien - bisher

- Dokumentation in der Verfahrensfreigabe (BayDSG)
- Technische Dokumentation, Datenschutzkonzept
- Regelungen zur Auftragsdatenverarbeitung, Fernwartung

Beispiel: Fragebogen

- Fragebogen zur Verwendung von BYOD, Cloud

·Der·Bayerische·Landesbeauftragte·für·den·Datenschutz·

Fragenbogen·zur·Nutzung·von·mobilen·Geräten·und·Cloud·Computing

Smartphones·(iPhone,·Android,·Windows·Phone),·Tablet-PCs

1)→Werden·Smartphones·oder·Tablet-PCs·als·Dienstgeräte·bereitgestellt·oder·ist·dies·geplant?

a)→Für·welche·Einsatzgebiete·und·Zwecke·werden·die·Geräte·genutzt?

b)→Ist·ein·Zugriff·auf·das·KIS·möglich?·Kann·auf·die·E-Mail-Postfächer·zugegriffen·werden?

c)→Werden·medizinische·Apps·auf·den·Geräten·verwendet?·Welche?

d)→Werden·personenbezogene·medizinische·Daten·auf·dem·Gerät·gespeichert·(evtl.·auch·nur·temporär)?

BYOD

2)→Dürfen·Privatgeräte·für·dienstliche·Zwecke·oder·den·Zugriff·auf·Daten·des·Krankenhauses·verwendet·werden·(BYOD)·oder·ist·dies·geplant?

a)→Für·welche·Einsatzgebiete·und·Zwecke·werden·die·Geräte·genutzt?

b)→Ist·ein·Zugriff·auf·das·KIS·möglich?·Kann·auf·die·E-Mail-Postfächer·zugegriffen·werden?

c)→Werden·medizinische·Apps·auf·den·Geräten·verwendet?·Welche?

d)→Werden·personenbezogene·medizinische·Daten·auf·dem·Gerät·gespeichert·(evtl.·auch·nur·temporär)?

e)→Welche·Nutzergruppen·dürfen·Privatgeräte·verwenden?·Welche·vertraglichen·Regelungen·hierzu·werden·getroffen?

f)→Wie·erfolgt·die·Trennung·zwischen·dienstlicher·und·privater·Nutzung?

Beispiel Fragebogen

- Versand Anschreiben und Fragebogen mit Fristen für Beantwortung
- Auswertung der Rückläufe
- Mitteilung von Mängeln und Anforderungen zur Behebung
- Eventuell Vor-Ort-Überprüfung der Behebung der Mängel

Beispiel: Vor-Ort-Prüfung

- Prüfung Berechtigungskonzept
  - Checkliste mit Fragen
  - Vorlage der Dokumentation des Berechtigungskonzepts
  - Vorlage der Anträge auf Benutzerkennungen und Berechtigungen
  - Einsichtnahme in das KIS an diversen Arbeitsplätzen (Pflege, Arzt, Sekretariate, Abrechnung / Controlling, Labor
    - Abrufbare Patienten
    - Abrufbare Organisationseinheiten, Abteilungen
    - Sperrung von Vorbehandlungen
    - Möglichkeiten für Notfallzugriffe

Beispiel: Protokollierung

- Anlassbezogen: Patient hat den Verdacht, dass seine Daten unbefugt eingesehen wurden
- Auswertung der Protokollierung der Zugriffe auf die Daten des Patienten
  - Welche Benutzerkennungen
  - Welche Zeitpunkte
  - Welche Operationen im KIS

Beispiel: Protokollierung

- Regelmäßige Auswertung in Stichproben
  - Zugriffe auf VIPs, Opfer von Katastrophen
  - Zugriffe nachts, am Wochenende
  - Häufigkeit von (Notfall-)Zugriffen
  - Eingegebene Begründungen bei Notfallzugriffen

Beispiel: Studien

- Meist Vorabprüfung z.B. auf Anforderung der Ethikkommission
- Prüfung Patienteninformation und Einwilligungserklärung
- Prüfung Datenschutzkonzept
  - Pseudonymisierungsverfahren, Risiken einer unbefugten Reidentifizierung
  - Verfahren zur (automatisierten) Auswahl von Patienten für Studien
  - Datenlöschung
  - Sichere Datenübermittlung

Änderungen durch die DSGVO

DSGVO legt größeren Schwerpunkt auf Technik:

- Art. 5 Abs. 1 Buchst. f DSGVO "Grundsätze für die Verarbeitung personenbezogener Daten",
- Art. 24 DSGVO "Verantwortung des für die Verarbeitung Verantwortlichen",
- Art. 25 DSGVO "Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen",
- Art. 32 DSGVO "Sicherheit der Verarbeitung",
- Art. 35 DSGVO "Datenschutz-Folgenabschätzung",
- Art. 36 DSGVO "Vorherige Konsultation".

https://www.datenschutz-bayern.de/datenschutzreform2018/

Änderungen durch die DSGVO

- Rechenschaftspflicht, Datenschutzmanagement
  - Art. 5 Abs. 2 DSGVO
  - Art. 24 Abs. 1 Satz 1 DSGVO
- Risikobasierter Ansatz hinsichtlich der Rechte und Freiheiten natürlicher Personen
- Meldung von Datenschutzverletzungen, Art. 33 DSGVO
- Zertifizierung

Technische Kriterien DSGVO

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Data protection by design/Datenschutz durch Technikgestaltung
- Data protection by default/datenschutzfreundliche Voreinstellungen
- Pseudonymisierung
- Verschlüsselung

Data protection by design / default

- Verhinderung von doppelter Datenspeicherung, z.B. auf medizinischen Geräten
- Möglichkeit zur Datenlöschung / Aussonderung
- Umsetzung von Berechtigungskonzepten in Subsystemen
- Vorkonfiguration von E-Mail-Servern, Gateway-zu-Gateway-Verschlüsselung
- Datenschutzfreundliche Konfiguration für mobile Geräte (Verschlüsselung, Container, Virtualisierung)
- Verschlüsselte Kontaktmöglichkeiten

DSFA

- Papiere DSK, Art. 29 – Gruppe, DKG
- Mindestinhalt:
  - Systematische Beschreibung der Verarbeitungsvorgänge, Zweck, Verantwortlicher
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung
  - Bewertung der Risiken für die Betroffenen
  - Technisch-organisatorische Abhilfemaßnahmen
  - Einholung von Meinungen von Betroffenen und bDSB
- Mehrere Methodiken denkbar, z.B. Standard-Datenschutz-Modell (SDM), PIA-Frameworks

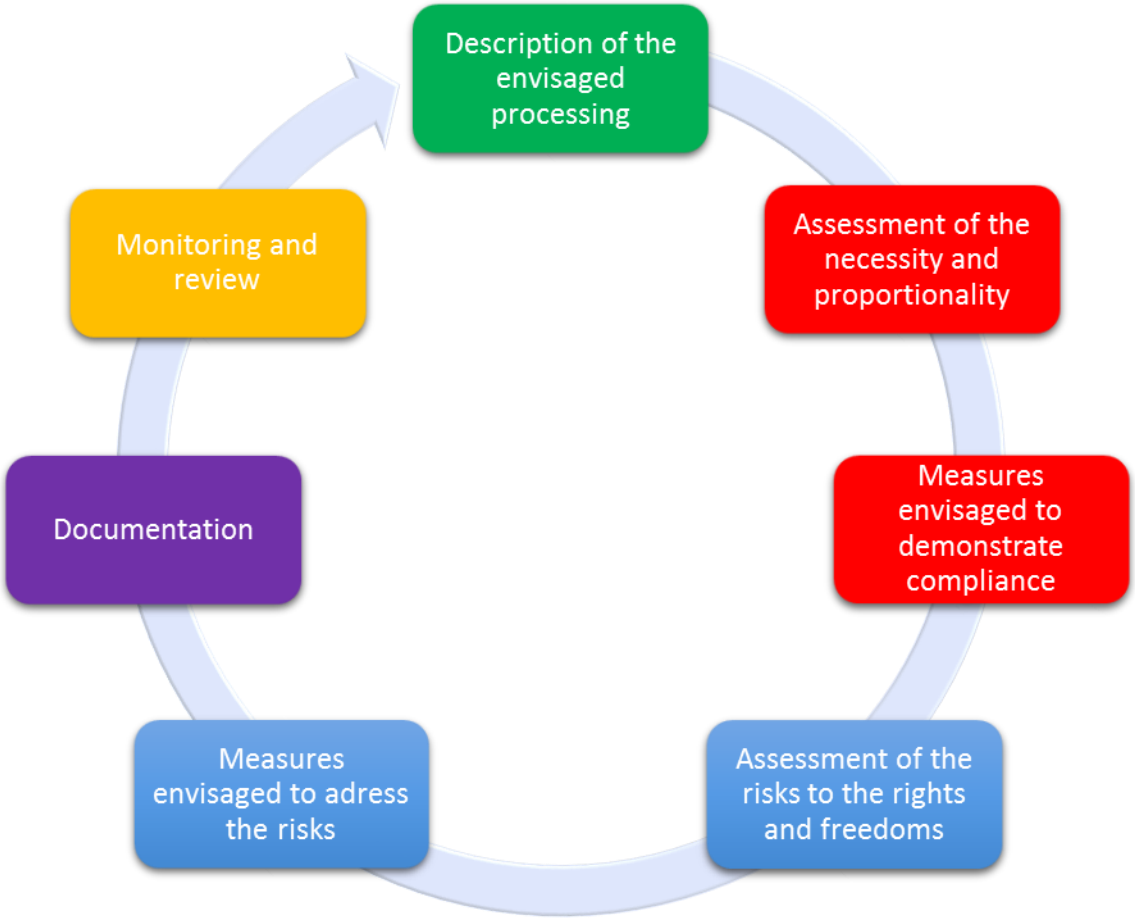
Hohes Risiko

- Bei zwei oder mehr der folgenden Kriterien:
  - Scoring, Profilbildung
  - Automatisierte Entscheidungen
  - Systematische Überwachung
  - Sensible Daten gemäß Art. 9 DSGVO
  - Datenverarbeitung in großem Umfang
  - Verknüpfung von Datensätzen unterschiedlicher verantwortlicher Stellen zu neuen Zwecken
  - Daten von besonders schützenswerten Personengruppen (z.B. Kinder, psychisch Kranke, Ältere)
  - Einsatz neuer Technologien
  - Beschränkung der Rechte der Betroffenen, eingeschränkter Zugang

Risikoanalyse

- Erfassung der bedrohten Objekte
- Bestimmung der Bedrohungen
- Erfassung des Täterkreises
- Suche nach Schwachstellen, d.h. Anwendbarkeit der Bedrohungen auf die Systeme
- Beurteilung
  - Schwere des Schadens
  - Eintrittswahrscheinlichkeit
  - Abhilfemaßnahmen zur Reduzierung des Risikos

DSFA



Quelle: Papier Art. 29 Gruppe

Datenschutzverletzungen

- Zumeist auch Problem der IT-Sicherheit
  - Gegen Vertraulichkeit: Hacking von Accounts, unbefugte Einsichtnahme z.B. Unbefugte Nutzung von Notfallzugriffsfunktionen, Verlust von Daten, Keylogger, Viren, Trojaner
  - Gegen Integrität: Verfälschung von Daten, fehlende Zurechenbarkeit von Dokumenten bei Gruppenkennungen
  - Gegen Verfügbarkeit, z.B. Verschlüsselungs-Trojaner, Viren, DoS, Systemausfälle
- Verfahren zum Erkennen und Behandeln von Verstößen

Datenschutzverletzungen

- Meldung an die Aufsichtsbehörde unverzüglich, möglichst binnen 72 Stunden
- Ausnahme: Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen
- Auftragsverarbeiter müssen an den Verantwortlichen melden

Datenschutzverletzungen

- DSGVO legt fest, was zu melden ist
  - Art der Verletzung
  - Betroffene personenbezogene Daten, insbesondere besondere Kategorien
  - Folgen der Verletzung
  - Beschreibung der ergriffenen oder geplanten Maßnahmen
  - Information der Betroffenen
- Online-Formular: https://www.datenschutz-bayern.de/service/data_breach.html

Erste Prüfungen nach DSGVO

- Einrichtung Datenschutzmanagement
  - Team für das Datenschutzmanagement
  - Meldungen bDSB
  - Verzeichnis der Verarbeitungstätigkeiten
  - Erfassung und Meldung von Datenschutzverletzungen
  - Übersicht Verträge Auftragsverarbeitung, Dienstleister
  - Risikoabschätzung, Vorbereitungen DSFA
  - Übersicht Datenschutzkonzepte
  - Umsetzung Auskunftsrechte, Akteneinsicht,
- Leitfaden: https://www.datenschutz-bayern.de/datenschutzreform2018/

Vielen Dank für Ihre Aufmerksamkeit

www.datenschutz-bayern.de

Bereiche Gesundheitswesen, Technik und
Tätigkeitsbericht, Datenschutzreform 2018