kbo
Zuverlässig an Ihrer Seite

Prüfaufgaben des Datenschutzbeauftragten

Agenda

1. Rechtliche Anforderungen
   - Aufgaben des Datenschutzbeauftragten
   - Rechenschaftspflichten aus der Datenschutzgrundverordnung (DSGVO 2018)
   - Kontrollpflichten aus der DSGVO
   - Datenschutzmanagementsystem
   - Zertifizierung im BDSG und in der DSGVO

2. Datenschutz-Organisation

3. Datenschutzprüfungen
   - Prüfungsplanung
   - Prüfungsdurchführung
   - Dokumentation
   - Zusammenarbeit einzelner Bereiche

über mich

Seit ca. 20 Jahren im Datenschutz tätig

Ausgebildet beim Landesamt für Datenschutz und Statistik in München

Konzerndatenschutzbeauftragter bei kbo

Externen Datenschutzbeauftragter in sozialen Einrichtungen

„Grundausbildung“ Betriebswirtschaft und Interne Revision

Stellv. Vorstandsvorsitzender beim Berufsverband der Datenschutzbeauftragten in Deutschland BvD e.V.

über kbo






- Verbund von Kliniken und ambulanten Einrichtungen für Psychiatrie, Psychotherapie und Psychosomatik für Kinder, Jugendliche und Erwachsene, Neurologie und Sozialpädiatrie
- 7.200 Mitarbeiter – etwa 110.000 Patienten jährlich
- stationäre, teilstationäre und ambulante Leistungen - wohnortnah in ganz Oberbayern an über 30 Standorten

Rechtliche Anforderungen

Aufgaben des Datenschutzbeauftragten

- Art. 39 DSGVO:
    - Abs. 1 lit. b): Überwachung der Einhaltung dieser Verordnung
    - Abs. 1 lit. c): Beratungs- und Überwachungsfunktion bei Datenschutzfolgeabschätzungen (Art. 35 DSGVO)
    - Abs. 1 lit. d+e): Zusammenarbeit mit Aufsichtsbehörden
    - Abs. 2: Durchführung einer eigenen Risikoeinschätzung zur Berücksichtigung des mit den Verarbeitungsvorgängen verbundenen Risikos bei der Erfüllung seiner Aufgaben
- Art. 38 DSGVO:
    - Abs. 6: Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Rechtliche Anforderungen

Rechenschaftspflichten aus der DSGVO

- Art. 5 Abs. 2 DSGVO: Der für die Verarbeitung Verantwortliche muss die Einhaltung der Datenschutz-Grundsätze nachweisen können
  - Rechtmäßigkeit
  - Verarbeitung nach Treu und Glauben
  - Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität & Vertraulichkeit

- Zur Erfüllung der Rechenschaftspflicht:
  Dokumentation des DSB über wesentliche Tätigkeiten seiner Person, bzw. seiner Mitarbeiter in einem zentralen Dokumentationstool (IDW PH 9.860.1)

Rechtliche Anforderungen

Kontrollpflichten aus der DSGVO

- Art. 24 Abs. 1 DSGVO: Der Verantwortliche setzt unter Berücksichtigung
  - der Art und des Umfangs,
  - der Umstände,
  - der Zwecke der Verarbeitung,
  - sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten

  geeignete technische und organisatorische Maßnahmen um und überprüft diese

- Art. 32 Abs. 1 DSGVO:
  Kein Höchstmaß an technischen und organisatorischen Maßnahmen, sondern, nach dem Stand der Technik, dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessene Maßnahmen
  - Abs.1 d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit

Rechtliche Anforderungen

Datenschutzmanagementsystem

Zur Erfüllung der gesetzlichen Anforderungen ist die Implementierung eines Datenschutzmanagement-Systems unerlässlich

Rechtliche Anforderungen

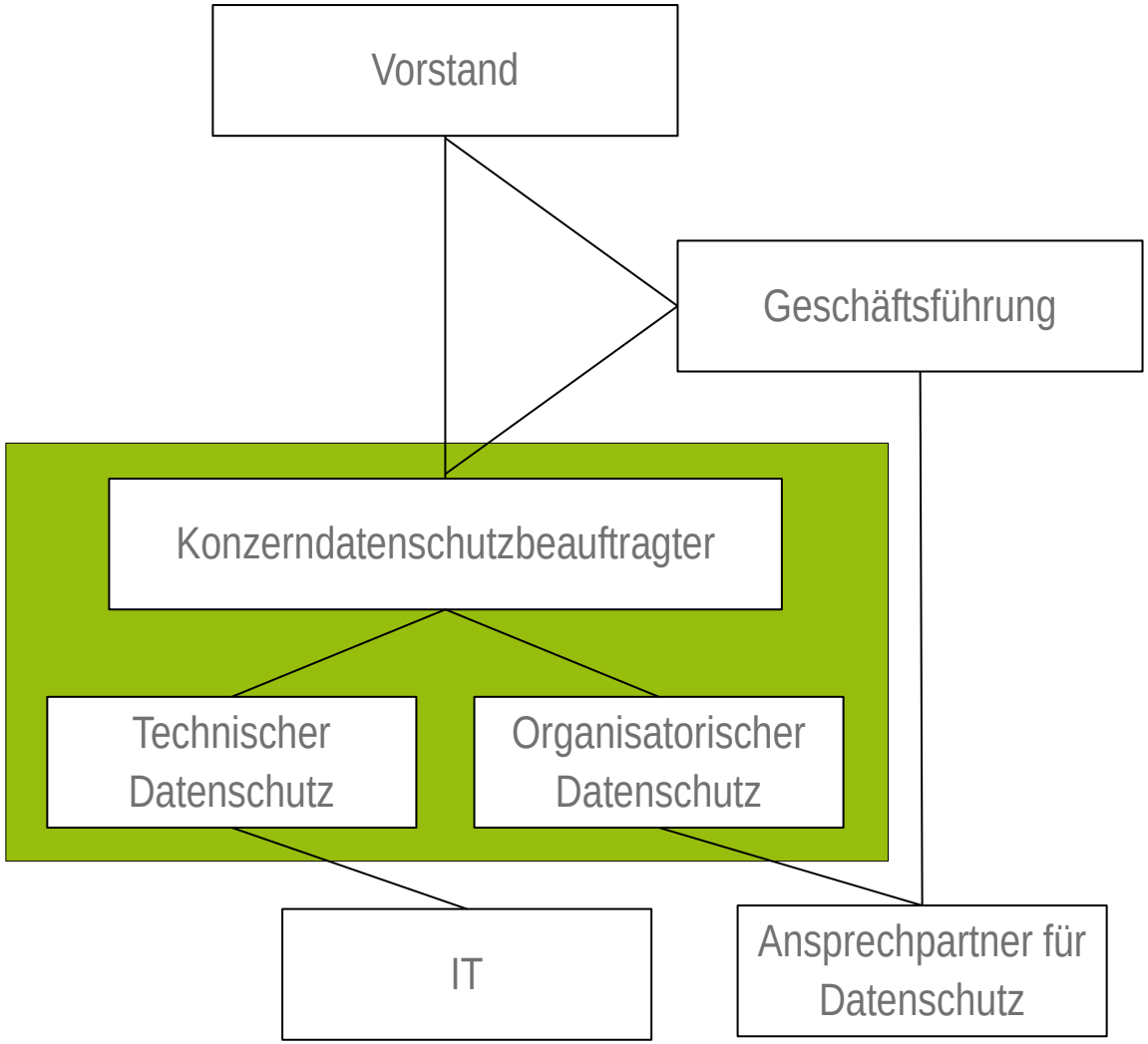
Zertifizierung im BDSG und in der DSGVO

Bereits im BDSG Forderung nach einer Zertifizierung:

- §9a BDSG :
  Zur Verbesserung des Datenschutzes & der Datensicherheit kann das Datenschutzkonzept und die technischen Einrichtungen durch unabhängige und zugelassene Gutachter überprüft und bewertet werden

- Art. 42 DSGVO:
  Schafft die Möglichkeit, mit der Einhaltung eines zertifizierten Genehmigungsverfahrens die Erfüllung der Anforderungen der DSGVO nachzuweisen
    - Bislang kein anerkanntes Zertifizierungsverfahren
    - ISO 27001 / 27701 wichtiger Schritt zu pragmatischen und zertifizierbaren Datenschutz

Datenschutz-Organisation



Konzerndatenschutz-Team

- Beratung
- Überwachung

Datenschutz-Organisation

Technischer Datenschutz

Aufgaben:

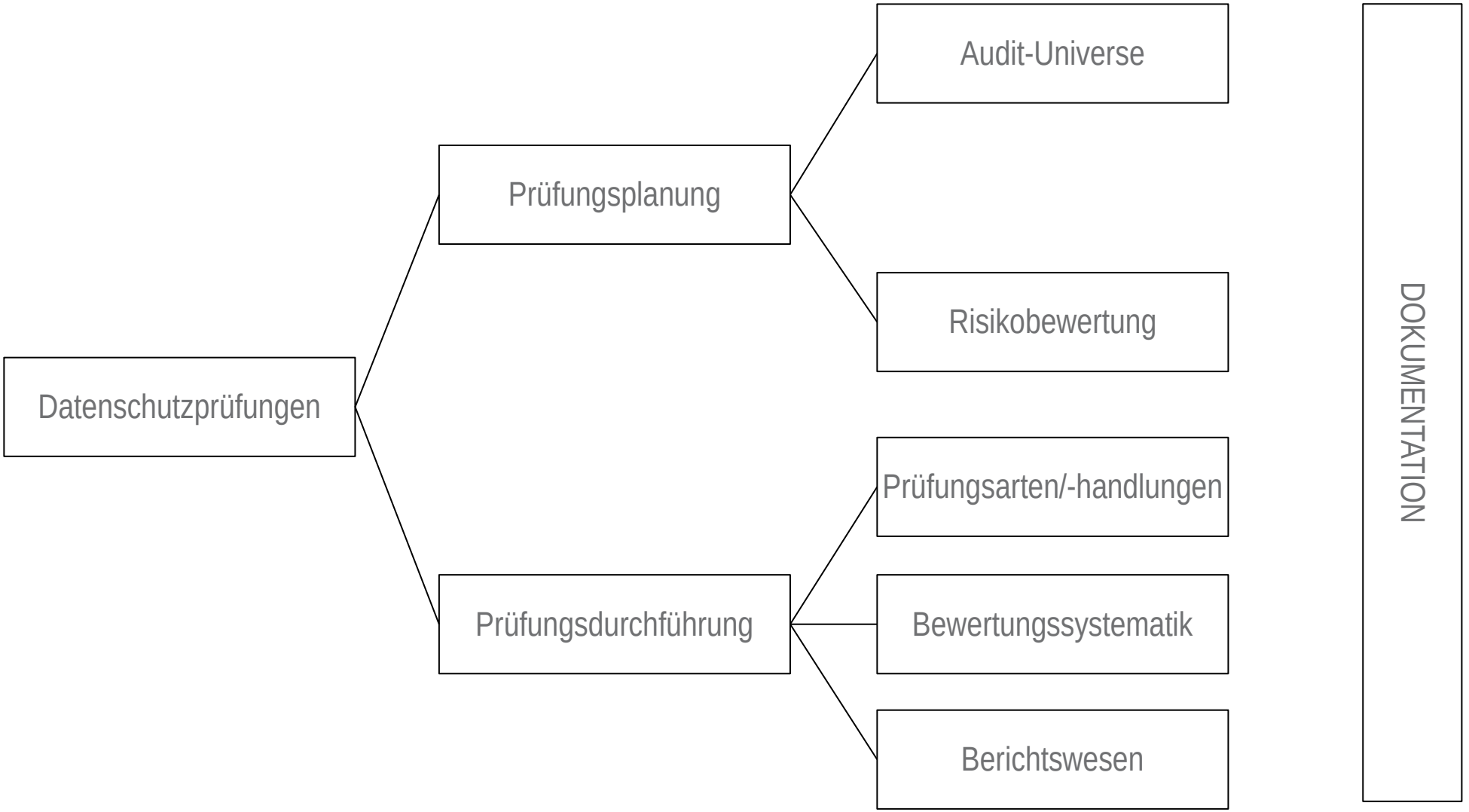
- Datenschutzfolgeabschätzung
- Verzeichnis von Verarbeitungstätigkeiten
- Rechte- und Rollen-Konzept
- …

Organisatorischer Datenschutz

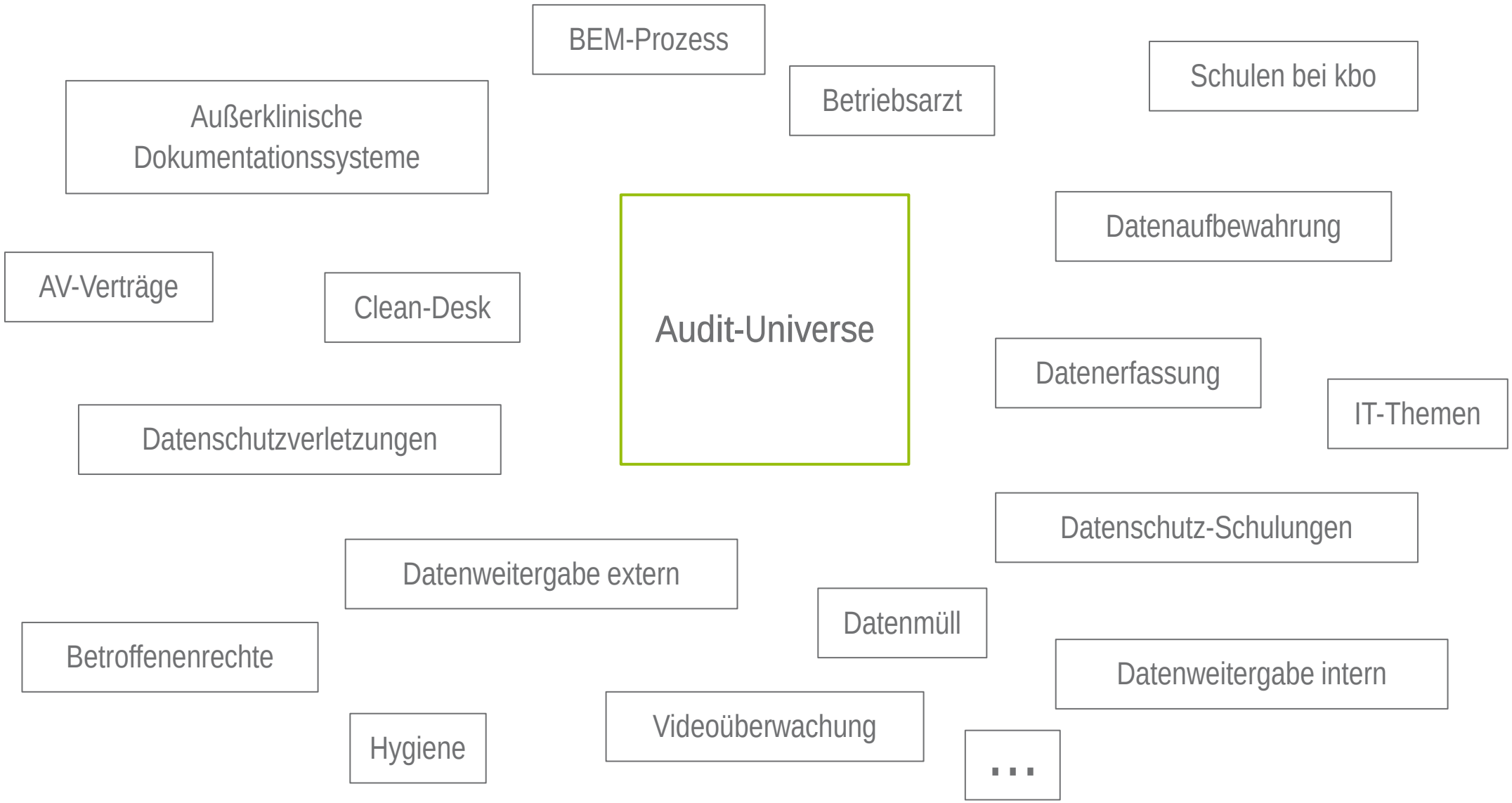
Aufgaben:

- Betroffenenrechte
- Auftragsverarbeitungsverträge
- Dokumentensteuerung
- …

Datenschutz-Prüfungen



Datenschutz-Prüfungen – Prüfungsplanung



Datenschutz-Prüfungen – Prüfungsplanung

kbo
Zuverlässig an Ihrer Seite

Risikobewertung

z.B. anhand folgender Kriterien:

- Zeitpunkt letzter Prüfung
- Brutto-Risiko laut Datenschutzfolgenabschätzung
- Höchste betroffene Datenschutzklasse
- Ergebnis letzter Prüfung
- Anzahl von Datenschutzmeldungen in den letzten 12 Monaten in diesem Prozess
- Schnittstellen im Prozess

Datenschutz-Prüfungen – Prüfungsplanung

kbo
Zuverlässig an Ihrer Seite

Zeitpunkt der letzten Prüfung	(1) weniger als 2 Jahre her (2) länger als 2 Jahre her	(3) länger als 5 Jahre her (4) länger als 10 Jahre her
Brutto-Risiko laut DSFA	(1) keine DSFA/ gering (2) mittel	(3) hoch (4) sehr hoch
Höchste betroffene Datenschutzklasse	(1) max. Klasse 4 oder 5 (2) Datenschutzklasse 3	(3) Datenschutzklasse 2 (4) Datenschutzklasse 1
Ergebnis der letzten Prüfung	(1) keine Prio1-Feststellung (2) 1-2 Prio1-Feststellungen	(3) 2< Prio1-Feststellungen
Anzahl Datenschutz-meldungen im Prozess	(1) 0-2 (2) 2-4/ keine	(3) ab 5
Anzahl Schnittstellen im Prozess	(1) keine (2) bis 2	(3) ab 3

Datenschutz-Prüfungen – Prüfungsplanung

kbo
Zuverlässig an Ihrer Seite

Risikoorientierte Prüfungsplanung

z.B. aufgrund vorangegangener Risikobewertung

- Die einzelnen Werte werden für jedes Prüffeld je nach Auswahl miteinander multipliziert, so dass sich ein Wert zwischen 1 und 1728 ergibt.
- Der erreichte Wert entscheidet darüber, welche Prüffelder in der Prüfungsplanung priorisiert werden.
- Es werden für jedes Jahr drei Prüfungen aus den Prüffeldern ausgewählt.
  (z.B. zwei Prüfungen mit Wert 96≤, eine Prüfung mit Wert <96)

Datenschutz-Prüfungen – Prüfungsdurchführung

Prüfungsdurchführung

Kick – Off

Prüfungsarten

- Prozessprüfung
- Einzelfallprüfung
- Begehung*
- Follow-Up-Prüfung (Maßnahmennachverfolgung)
- Sonderprüfungen (v.a. bei Datenschutzverstößen)

Prüfungshandlungen

- Bestätigen von Sachverhalten durch externe Parteien
- Analyse von Dokumenten
- Stichprobenprüfungen
- analytische Prüfungshandlungen (Auswertungen)
- exemplarischer Prozessdurchlauf
- direkte Beobachtung
- Interviews

Abschlussbesprechung

* Prüfungen, bei denen bestimmte Standardprüffelder in regelmäßigen Abständen vor Ort und stichprobenhaft kontrolliert werden.

Datenschutz-Prüfungen – Prüfungsdurchführung

kbo
Zuverlässig an Ihrer Seite

Bewertungssystematik von Prüfungsfeststellungen

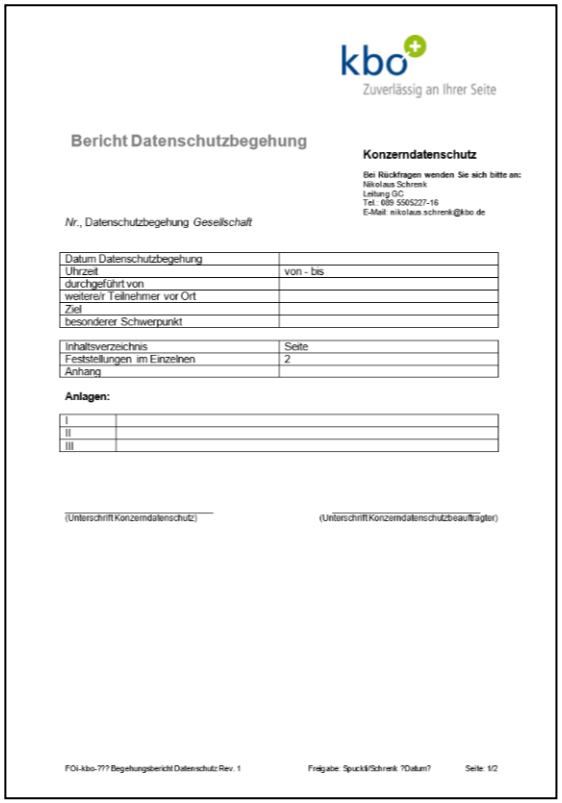
z.B. Festlegung von Prioritäten

Priorität 1	Es wird eine gesetzliche Vorschrift nicht eingehalten bzw. es besteht aktuell ein sehr hohes Risiko. Es sind umgehend Maßnahmen einzuleiten, um den Verstoß abzustellen.
Priorität 2	Es wird eine interne Vorgabe nicht eingehalten. Die derzeitige Geschäftsabwicklung kann zu einem hohen Unternehmensrisiko führen.
Priorität 3	Es wird eine interne Vorgabe nicht eingehalten. Mit der Nichteinhaltung ist ein niedriges Unternehmensrisiko verbunden.
Priorität 4	Es sind Verbesserungen in der Unternehmensabwicklung möglich, diese sind bei einer Neugestaltung bzw. Änderung von Prozessen zu berücksichtigen.

Datenschutz-Prüfungen – Prüfungsdurchführung

Berichtswesen

- Prüfungsbericht
  vom Vorstand zu unterschreiben
  Maßnahmen sind umzusetzen
- Begehungsprotokoll
  keine Unterschrift des Vorstands
  oder Geschäftsführers
- Stellungnahmen
  (v.a. bei Sonderprüfungen)
- Jahresbericht
  Tätigkeiten des Jahres



kbo
Zuverlässig an Ihrer Seite

Bericht Datenschutzbegehung

Konzerndatenschutz

Bei Rückfragen wenden Sie sich bitte an:
Nikolaus Schrenk
Leitung GC
Tel.: 089 5505227-16
E-Mail: nikolaus.schrenk@kbo.de

Nr., Datenschutzbegehung *Gesellschaft*

Datum Datenschutzbegehung	
Uhrzeit	von - bis
durchgeführt von	
weitere/r Teilnehmer vor Ort	
Ziel	
besonderer Schwerpunkt	

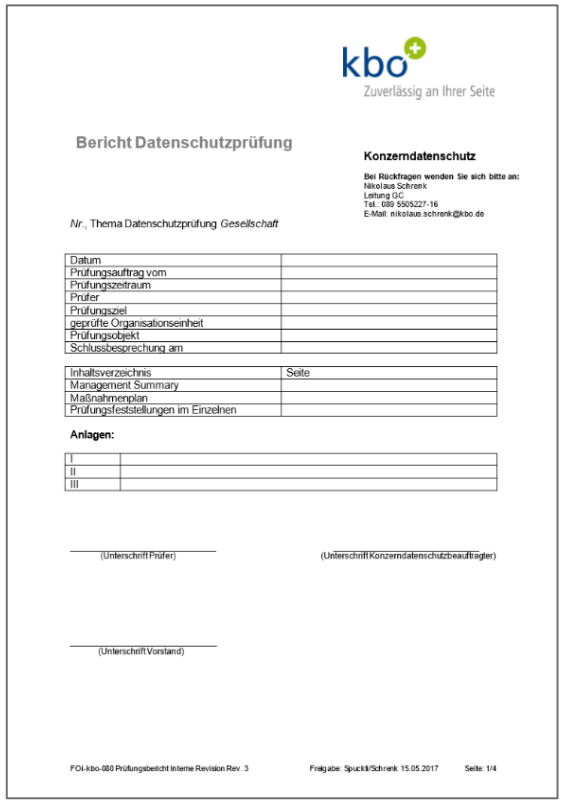
Inhaltsverzeichnis	Seite
Feststellungen im Einzelnen	2
Anhang	

Anlagen:

I	
II	
III	

(Unterschrift Konzerndatenschutz) (Unterschrift Konzerndatenschutzbeauftragter)

FOI-kbo-77? Begehungsbericht Datenschutz Rev. 1 Freigabe: Spuckl/Schrenk ?Datum? Seite: 1/2



kbo
Zuverlässig an Ihrer Seite

Bericht Datenschutzprüfung

Konzerndatenschutz

Bei Rückfragen wenden Sie sich bitte an:
Nikolaus Schrenk
Leitung GC
Tel.: 089 5505227-16
E-Mail: nikolaus.schrenk@kbo.de

Nr., Thema Datenschutzprüfung *Gesellschaft*

Datum	
Prüfungsauftrag vom	
Prüfungszeitraum	
Prüfer	
Prüfungsziel	
geprüfte Organisationseinheit	
Prüfungsobjekt	
Schlussbesprechung am	

Inhaltsverzeichnis	Seite
Management Summary	
Maßnahmenplan	
Prüfungsfeststellungen im Einzelnen	

Anlagen:

I	
II	
III	

(Unterschrift Prüfer) (Unterschrift Konzerndatenschutzbeauftragter)

(Unterschrift Vorstand)

FOI-kbo-080 Prüfungsbericht Interne Revision Rev. 3 Freigabe: Spuckl/Schrenk 15.05.2017 Seite: 1/4

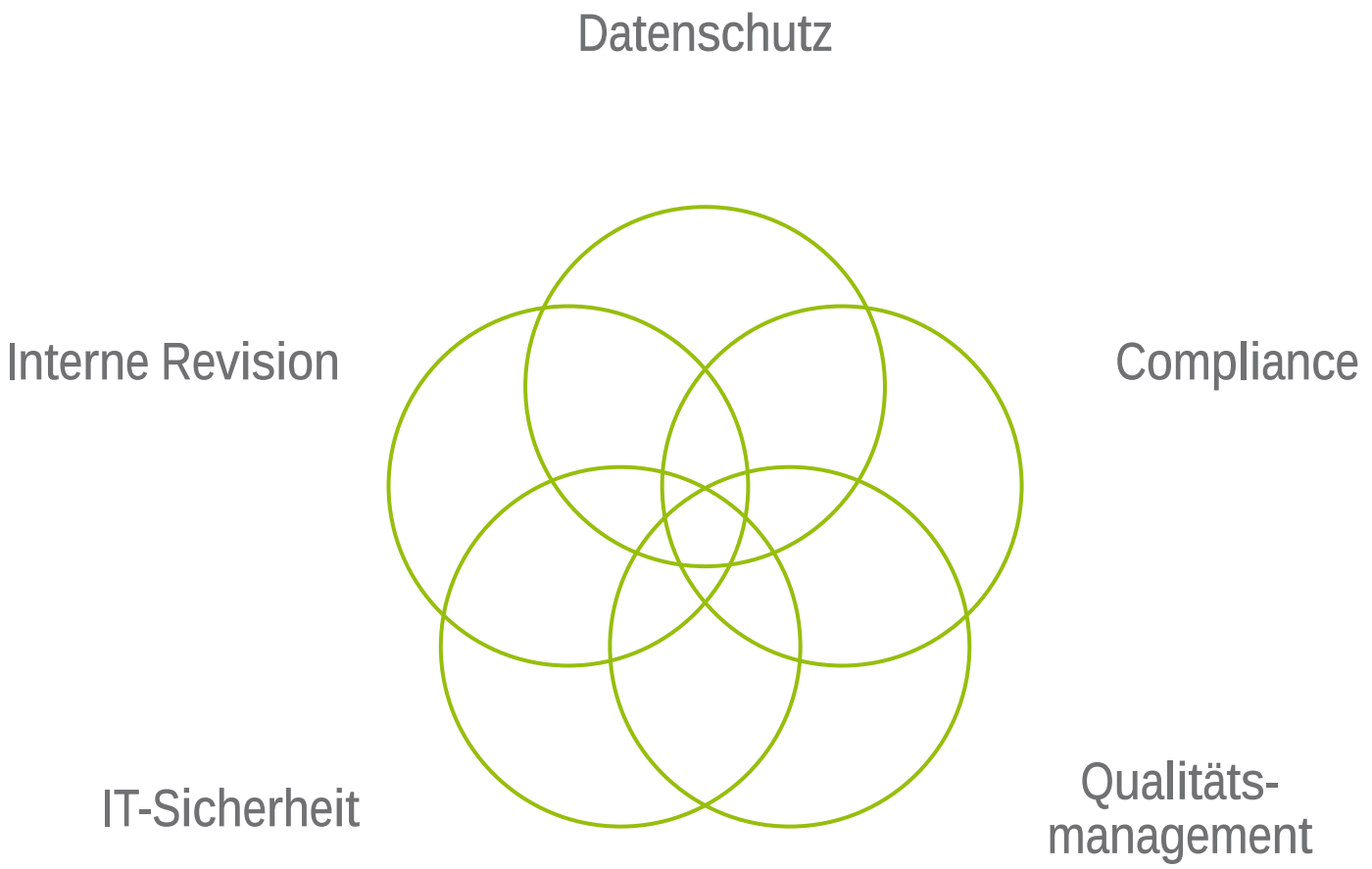
Dokumentation

Dokumentation von Datenschutzprüfungen

- Prüfungsplanung anhand von Audit-Universe und Risikobewertungssystem
- Prüfungsfeststellungen inkl. Nachverfolgungsprozess
- Ablage von relevanten Dokumenten zur Prüfung (Berichte, Nachweise, Richtlinien, etc.)

Ggf. Verwendung von Dokumentationstools, auch zur Sicherstellung der Rechenschaftspflichten

Zusammenarbeit einzelner Bereiche



z.B. gemeinsame Audits, Co-Sourcing

Fragen/Anmerkungen

Vielen Dank für Ihre

Aufmerksamkeit!

Für Fragen stehe ich Ihnen gerne zur Verfügung:

Nikolaus Schrenk
Kliniken des Bezirks Oberbayern – Kommunalunternehmen
Prinzregentenstraße 18
80538 München
E-Mail: nikolaus.schrenk@kbo.de
Telefon: 089 5505227-16