kbo
Zuverlässig an Ihrer Seite

Einführung eines Datenschutzmanagementsystems (DSMS)

Agenda

kbo
Zuverlässig an Ihrer Seite

1. **Hinweise in der DSGVO**
2. DSMS – Was ist das?
3. Einführung DSMS
4. Erfahrungen bei der Einführung eines DSMS
5. Fazit

Über mich / über kbo

Nikolaus Schrenk

- Stellv. Vorstandsvorsitzender Berufsverband der Datenschutzbeauftragten e.V.
- Vorstandsbereichsleiter Governance & Consulting bei den Kliniken des Bezirks Oberbayern
- Gastreferent Hochschule München, Fachbereich Mental Health

Kliniken des Bezirks Oberbayern

- Die Angebote der Kliniken des Bezirks Oberbayern (kbo) in den Bereichen Psychiatrie, Psychotherapie und Psychosomatik für Kinder, Jugendliche und Erwachsene, Neurologie und Sozialpädiatrie finden Sie an über 50 Standorten. kbo leistet rund um die Uhr eine Versorgung von hoher Qualität. Unsere Leistungen bieten wir stationär, teilstationär und ambulant an.
- Derzeit ca. 7.500 Mitarbeiter

Hinweise in der DSGVO

Art. 5 Abs. 2 DSGVO: Der für die Verarbeitung Verantwortliche muss die Einhaltung der Datenschutz-Grundsätze nachweisen können (Rechenschaftspflicht)

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität & Vertraulichkeit

Hinweise in 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 DSGVO: Sicherheit der Verarbeitung

- Abs.1 d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Hinweise in der DSGVO

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

Hinweise in der DSGVO

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

Agenda

kbo
Zuverlässig an Ihrer Seite

1. Hinweise in der DSGVO
2. **DSMS – Was ist das?**
3. Einführung DSMS
4. Erfahrungen bei der Einführung eines DSMS
5. Fazit

DSMS – Was ist das?

Methodik, um gesetzliche und betriebliche Anforderungen und Maßnahmen im Umgang mit personenbezogenen Daten strukturiert

- zu planen,
- durchzuführen,
- zu kontrollieren und
- weiterzuentwickeln.

Zentral: Nachweis der Umsetzung!

Beschreibung der Prozesse und Auditnachweise sind unumgägnlich

Agenda

kbo
Zuverlässig an Ihrer Seite

1. Hinweise in der DSGVO
2. DSMS – Was ist das?
3. **Einführung DSMS**
4. Erfahrungen bei der Einführung eines DSMS
5. Fazit

Einführung DSMS

kbo
Zuverlässig an Ihrer Seite

PLANUNG

Soll-Analyse

- Welche Gesetze gelten?
- Was fordern die Gesetze konkret?

Ist-Analyse

- Welche Datenschutzprozesse gibt es?
- Welche vorhandenen Strukturen/ Schnittstellen gibt es?

Organisation

- Welche Ressourcen werden benötigt?
- Welche Verantwortlichkeiten sind festzulegen?

Einführung DSMS – Soll-Analyse

- ✓ Betroffenenrechte (Art. 13 ff. DSGVO) inkl. Datenschutzverstöße (Art. 4 Nr. 12 DSGVO; Art. 33 Abs. 5 DSGVO)
- ✓ Verträge zur Auftragsdatenverarbeitung (Art. 28 DSGVO)
- ✓ Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- ✓ Löschkonzepte
- ✓ Technische und organisatorische Maßnahmen (Art. 32 Abs. 1 DSGVO)
  z.B. IT-Sicherheitskonzept, Schulungen zur Sensibilisierung von Mitarbeitenden,…
- ✓ Datenschutzprüfungen (Art. 32 Abs. 1 DSGVO)
- ✓ Datenschutzfolgenabschätzung (Art. 35 Abs. 2 DSGVO)

→ Definition von Soll-Werten in Datenschutzrichtlinie/-konzept inkl. Prozessbeschreibungen

Wsl. in Zukunft: Zertifizierung (Art. 42 und 43 DSGVO)

Einführung DSMS – Ist-Analyse

Verzeichnis der Verarbeitungstätigkeiten als Grundlage für DSMS

→ Definition von wichtigen Prozessen mit personenbezogenen Daten

Kontaktdaten Verantwortliche/r	Kontaktdaten Datenschutzbeauftragte/r

Name d. Verarbeitungs-tätigkeit	Zwecke d. Verarbeitung	Kategorien betroffener Personen	Kategorien betroffener Daten	Kategorien von EmpfängerInnen	Übermittlung Drittland	Löschfristen	TOMs
Personalver-waltung	…	…	…	…	…	…	…

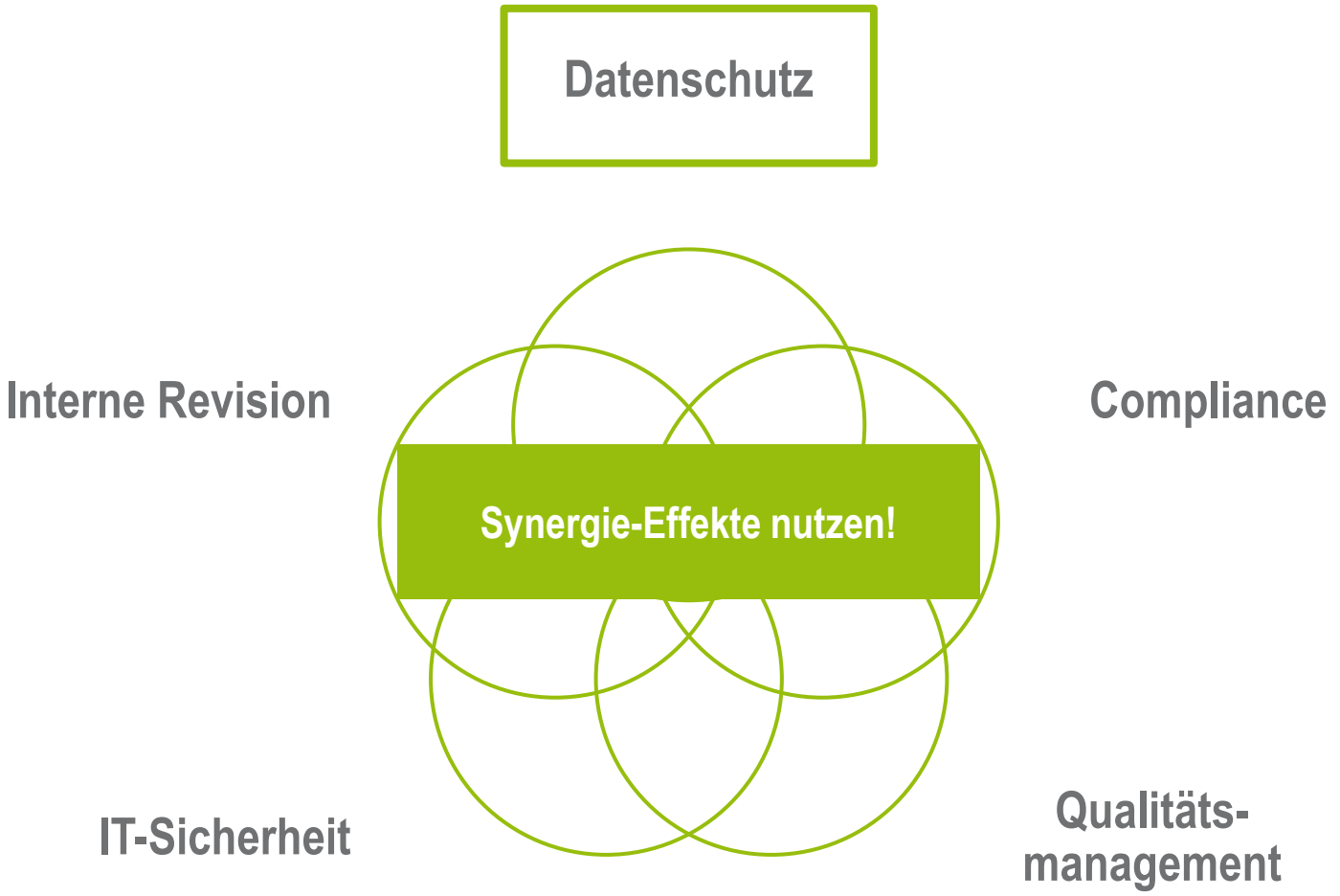
Prozessverantwortliche/r

Abteilungsleitung Personal

→ Zusätzliche Definition von prozessverantwortlichen Personen

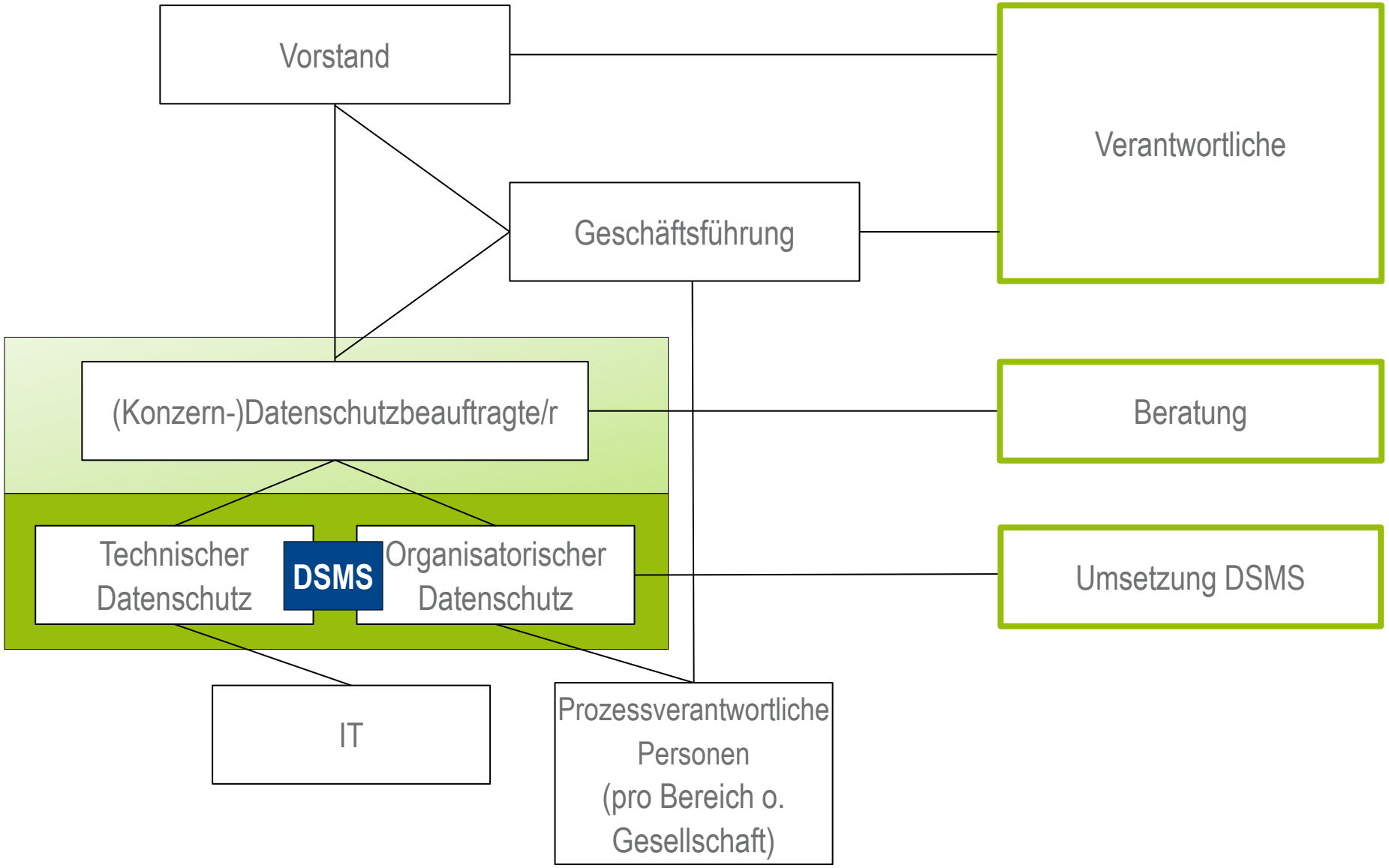
Einführung DSMS – Ist-Analyse

Einführung DSMS – Ist-Analyse



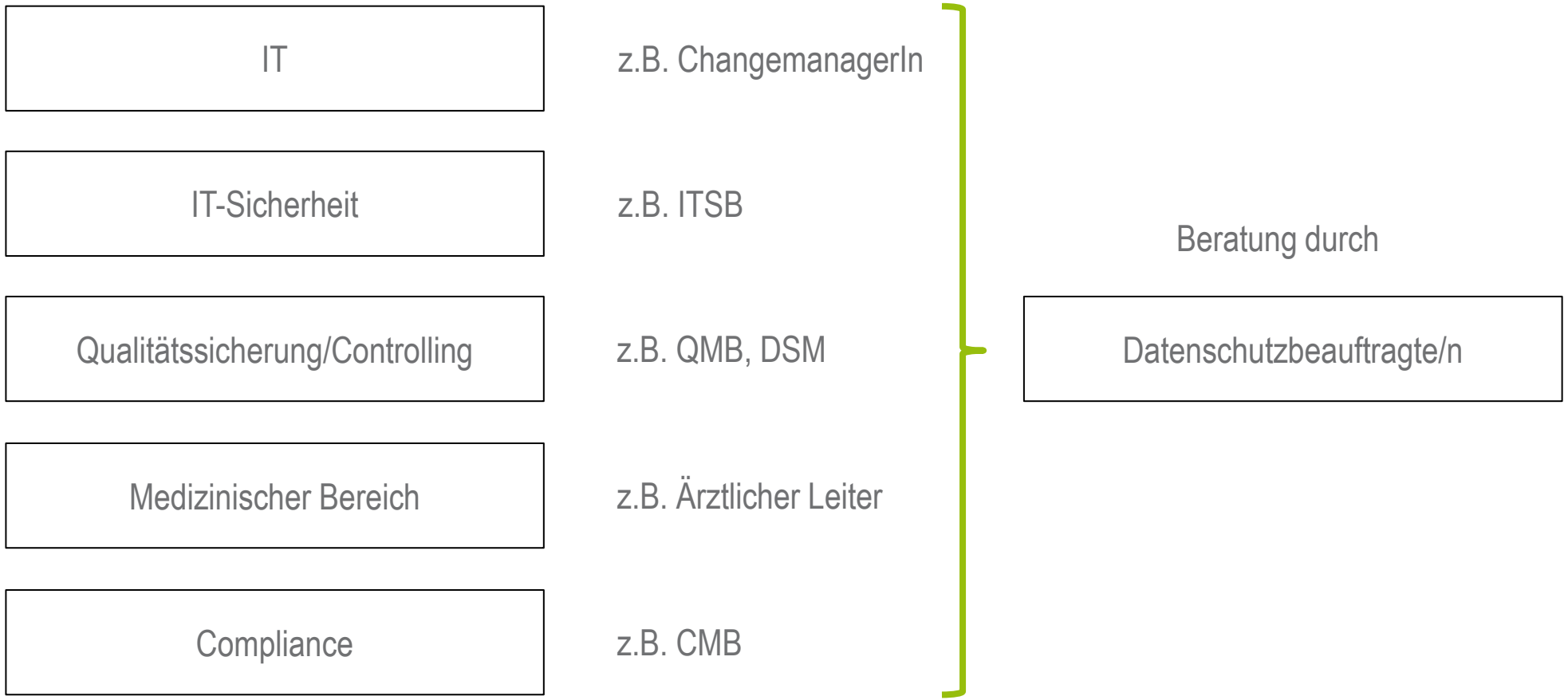
z.B. Nutzung vorhandener Strukturen (Software, Berichtswesen, etc.), …

Einführung DSMS – Organisation



Einführung DSMS – Organisation

1. Festlegung eines Datenschutz-Teams zur Umsetzung des DSMS aus den Bereichen…



Einführung DSMS – Organisation

kbo
Zuverlässig an Ihrer Seite

2. Festlegung von Rollen und Verantwortlichkeiten innerhalb des Datenschutz-Teams

IT	IT-Sicherheit	Compliance	Qualitätssicherung/ Controlling

Technischer Datenschutz:

- Datenschutz-Folgenabschätzung
- Verzeichnis von Verarbeitungstätigkeiten
- Rechte-Rollen-Konzept
- Löschkonzept
- …

Datenschutzbeauftragte/r

- Beratung beider Bereiche
- Übernahme zusätzl. Aufgaben z.B. Bearbeitung DS-Verletzungen

Organisatorischer Datenschutz:

- Betroffenenrechte inkl. DS-Verletzungen
- Auftragsverarbeitungsverträge
- Dokumentensteuerung
- Abstimmung mit medizinischen Bereichen
- Schulungen der MA in Zus.arbeit mit DSB
- …

Einführung DSMS

Zuverlässig an Ihrer Seite

Risikoorientierte Konzeption von Datenschutzmaßnahmen und -prozessen

Anpassung/ Verbesserung der Datenschutzprozesse

Standardisierung/ Implementierung von Datenschutzprozessen

Überprüfung des Datenschutzes bzw. der Maßnahmen

Agenda

kbo
Zuverlässig an Ihrer Seite

1. Hinweise in der DSGVO
2. DSMS – Was ist das?
3. Einführung DSMS
4. **Erfahrungen bei der Einführung eines DSMS**
5. Fazit

Erfahrungen bei der Einführung eines DSMS

kbo
Zuverlässig an Ihrer Seite

- Verzeichnis der Verarbeitungstätigkeiten als Grundlage für Einführung eines DSMS essentiell
- Viele Schnittstellen zu anderen Bereichen → Nutzung von Synergien möglich

  Aber auch: → Klare Festlegung von Rollen und Verantwortlichkeiten notwendig
- Veränderungen in Prozessen und Gesetzmäßigkeiten → Regelmäßiger Austausch mit verschiedenen Bereichen hilfreich (z.B. Compliance oder Interne Revision)
- Vieles bereits vorhanden (Risikomanagement, QM, Verzeichnis der Verarbeitungstätigkeiten, etc.) / korrekt gelebt → Anpassung DSMS an bereits vorhandene Strukturen
- Feststellen wichtiger Datenschutzprozesse (Datenschutz-Universe) → Ableitung von Überwachungs-, Schulungsthemen möglich
- Definition von Kennzahlen → Nachvollziehen der ständigen Weiterentwicklung möglich
- Enge Zusammenarbeit mit Datenschutzbeauftragten → Nutzung des Fachwissens hilfreich
- Orientierung an Anforderungen der Wirtschaftsprüfer → Analyse des Ist-Standes anhand IDW PH 9.860.1 möglich

Best Practice Methoden

- Fachbücher und Fachzeitschriften helfen
- Vorgehensmodell aus der ISO 27001 – Implimentierungs guides
- Vorgehensmodell aus der ISO 9001 – Plan – Do – Check- Akt Model – Wirksamkeitsmessung von Maßnahmen und Dokumentenlenkung
- Priorisierungsmodell vom Prozesses in der IT – COBIT Modell - Auswahl der wichtigen Prozesse aus der Strategie abgelegeit für den IT Betrieb

- Beratungsansatz: Der DSB muss aktiv die Zeit bekommen, um mit seinem Projektteam die verantwortlichen Stellen und die Prozess- Eigner zu beraten

- Software: kann wirklich helfen – steuert in gewissen Maße die Prozesse: aber: man kann sich auch in den Tools „verfangen“

Agenda

kbo
Zuverlässig an Ihrer Seite

1. Hinweise in der DSGVO
2. DSMS – Was ist das?
3. Einführung DSMS
4. Erfahrungen bei der Einführung eines DSMS
5. **Fazit**

Fazit

DSMS für alle Unternehmen sinnvoll, da es…

+ die Umsetzung der datenschutzrechtlichen Anforderungen und der Dokumentationspflicht strukturiert.

+ im Ernstfall bußgeldmindernd wirken kann.

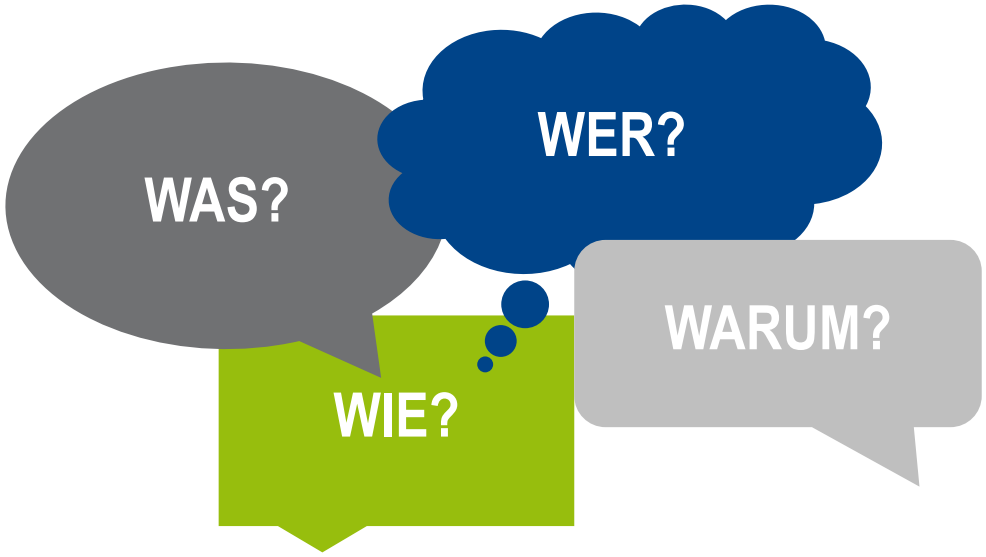
+ Übersichtlichkeit und kontinuierliche Prozessoptimierungen mit sich bringt.

+ ein angemessenes Datenschutzniveau für KundInnen und MitarbeiterInnen gewährleisten kann.

Ein guter Plan zur Einführung reichten den AB

um ein Bußgeld möglicherweise zu verhindern

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