

# ISMS-Einführung in Zürcher Spitäler

Ein Erfahrungsbericht

**vzk**



# Agenda

01

Zu beachtende  
Interessens- und  
Rechtsgebiete

02

Herausforderungen in  
Zürcher Spitälern -  
Vorgehen des VZK

03

Status Implementierung  
Zürcher Spitäler –  
2022 und heute

04

Cyberversicherungen  
und Standards  
(ISO27K & BSI)

05

Vorgehen x-tention

06

„Stand der Technik“  
als Rechtsbegriff

07

Dos & Don'ts

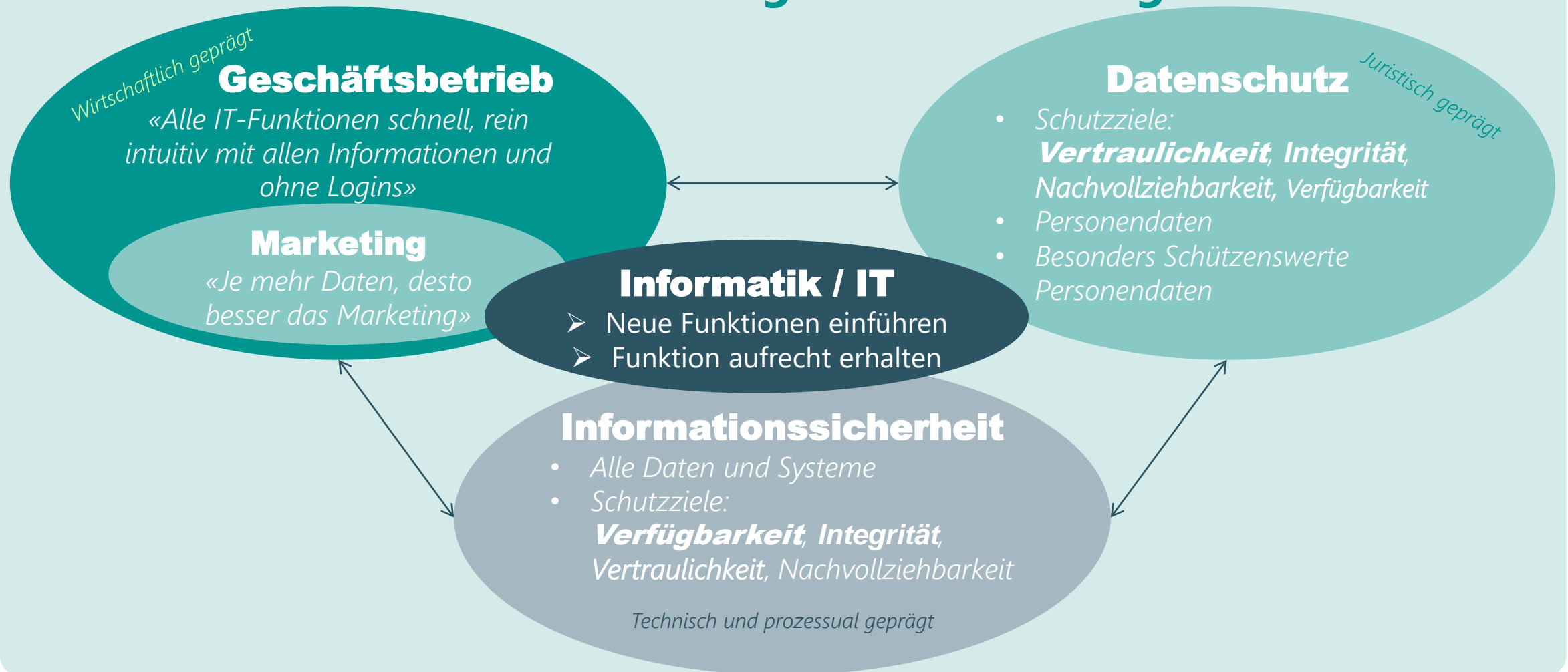
01

# Zu beachtende Rechtsgebiete

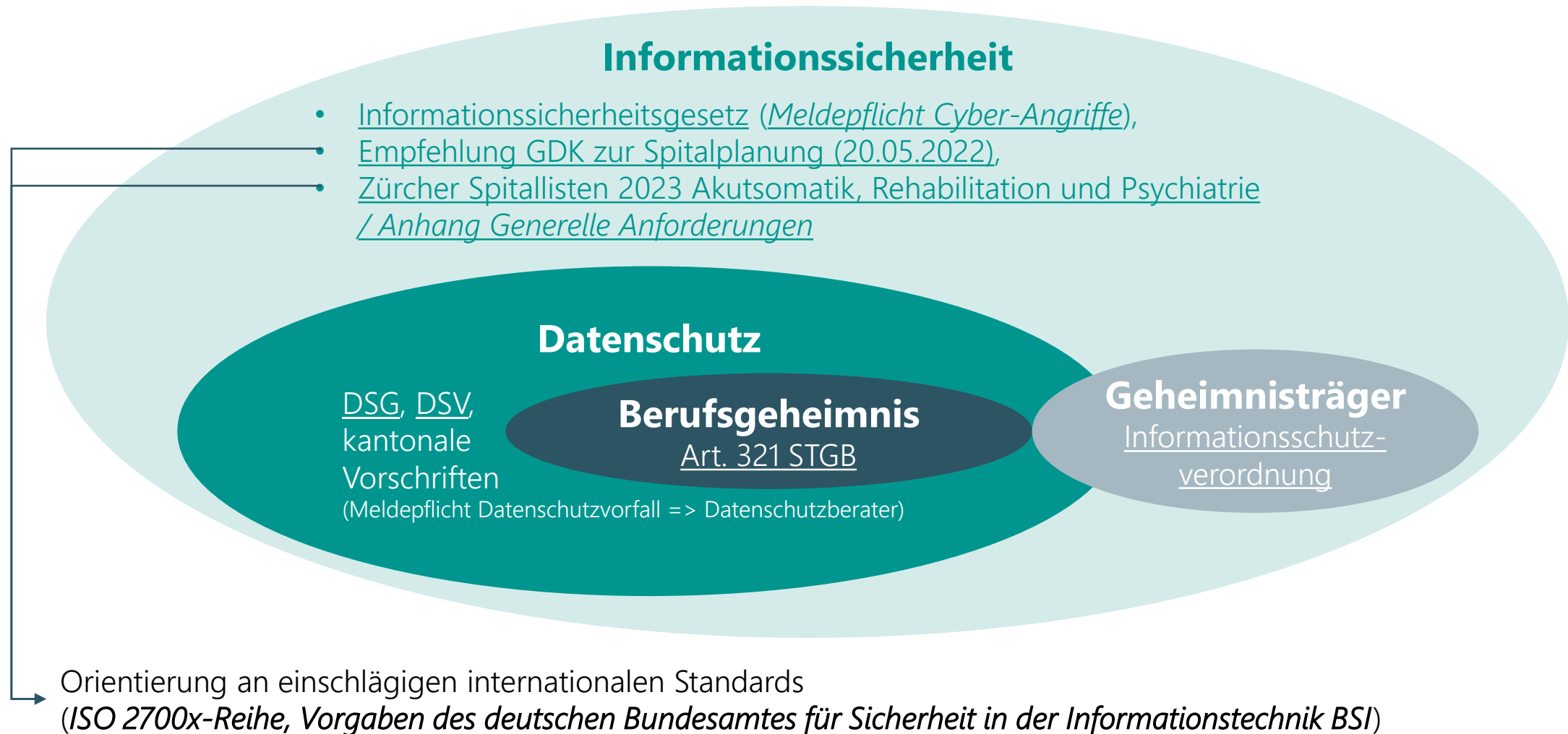
Änderungen mit steigender Kadenz

# Spannungsfeld – Interessenkonflikte

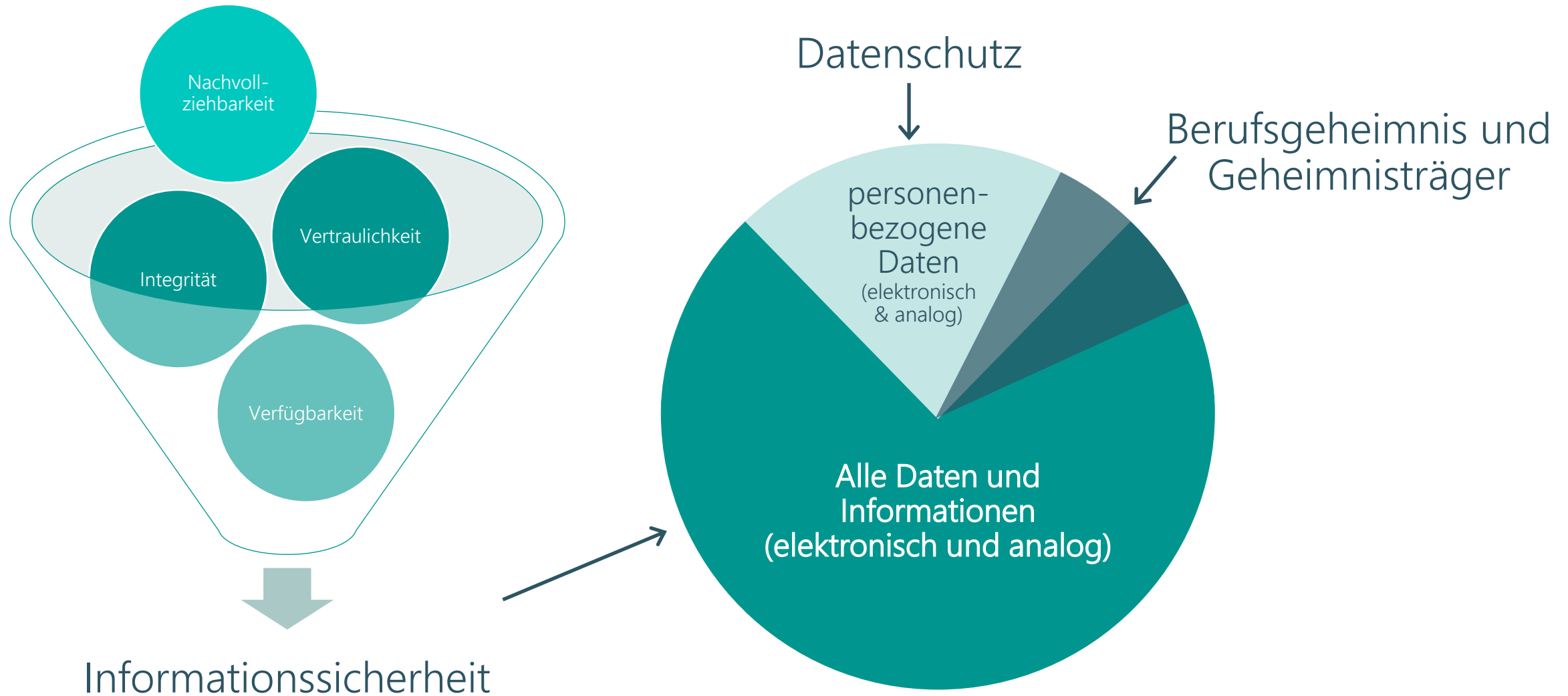
## Geschäftsleitungsverantwortung



# Pflichten in Informationssicherheit, Datenschutz, Berufsgeheimnis und Geheimnisträger



# Schutzziele bei Informationssicherheit, Datenschutz, Berufsgeheimnis und Geheimnisträger



# Rechtsquellen zum Nachschlagen

Umsetzung in Organisationsregelungen und fachspezifisches Rechtsmonitoring sind notwendig

- Berufsgeheimnis (*Schweiz*) [Art. 321 StGB](#), stabil, keine Änderungen seit Jahren
- Datenschutzrecht  
(*Kantone, Schweiz und Europa*) Schweiz, \**Neu*: [Datenschutzgesetz](#) und [Datenschutzverordnung](#), in Kraft ab 1.9.2023  
Europa: [DSGVO](#) und die sich entwickelnde Rechtsauffassung, in Kraft seit 25.5.2018
- Informationssicherheitsrecht  
(*Schweiz und Europa*) Schweiz, \**Neu*: [Informationssicherheitsgesetz](#), in Kraft ab 1.5.2022; NCSC Rechtsauffassung  
\**Zukunft*: Informationssicherheitsgesetz ([Meldepflicht Cyber-Angriffe](#))  
Schweiz, \**Neu*: [Empfehlung GDK zur Spitalplanung \(20.05.2022\)](#)  
Deutschland/Europa, \**Neu*: [KRITIS-Verordnung](#) Änderung, in Kraft seit 23.2.2023  
Deutschland/Europa, \**Neu*: [Informationssicherheit im Krankenhaus - Branchenspezifischer Sicherheitsstandard \(B3S\)](#), neue Version 8.12.2022
- Geheimnisträgerrecht  
(*Schweiz*) Schweiz: [Informationsschutzverordnung](#), in Kraft seit 1.10.2010  
Deutschland: [Sicherheitsüberprüfungsgesetz](#), in Kraft seit 5.7.2021
- Vertrags- und Lizenzrecht  
(*Schweiz und international*) Selbstgeschaffenes Recht in Verträgen; Akzeptanz von Lizenzverträgen  
GDK und Kanton Zürich: [Anhang generelle Anforderungen an Listenspitäler](#)
- Arbeitsrecht  
(*Schweiz*) Verantwortung des Vorgesetzten und der Geschäftsleitung für die Einhaltung von gesetzlichen Vorschriften - auch nach „Stand der Technik“ geeignete Arbeitsmittel zur Einhaltung der gesetzlichen Vorschriften für Mitarbeitende bereitzustellen

02

Herausforderungen in  
Zürcher Spitälern –  
Vorgehen des VZK



# Herausforderungen und Vorgehen im Verband Zürcher Krankenhäuser

GD ZH Anforderung an Listenspitäler: Einführung ISMS (Ausrichtung an ISO2700x , Vorgaben deutsches BSI)

VZK evaluiert kostengünstige Lösungspartner mit nachgewiesenen Erfahrungswerten bei Gesundheitseinrichtungen.



**Spitalleitung Verantwortung**  
erkennen und wahrnehmen

**Ressourcenengpässe**  
in IT, Datenschutz und Informationssicherheit - insbesondere bei mittleren und kleinen Spitälern

**Anwendungsbereiche**  
Welche Regularien sind für die Bereiche des Spitals anwendbar (Rechtsform, Leistungsaufträge)?

**GAP's in der Awareness**  
zu Informationssicherheit und Datenschutz in der Spitalbelegschaft (zeitgemässe Schulungskonzepte erforderlich)

- Don't**
  - eine grosse Schulung alle x Jahre
- Do**
  - Laufende Aufrechterhaltung der Awareness durch obligatorische 5 – 10 Minuten pro Monat
  - Inhalte, die praktisch zeigen, wie es richtig geht (Enablement der Mitarbeitenden)

**Informationssicherheit**

- Einbindung Partner (Outsourcing-Dienstleister, Handwerker, Personaldienstleister etc.):
  - Reglemente (Kenntnis, Bestätigung der Kenntnisnahme etc.),
  - Sicherheitsmanagementprozesse (Schnittstellen, Artefakte etc.),
  - Dokumentation (Servicearchitektur, Datenspeicherorte etc.)

**Datenschutz**

- Generelles Verständnis bei **allen** Mitarbeitenden (in- & externe)
- Abgrenzung Berufsgeheimnis – Datenschutz
- Richtiger Umgang bei Weitergabe, Benachrichtigung & Auskunft
- Verstehen der Herausforderungen bei Einwilligungen und Widerruf von Einwilligungen

**Datenschutz und Informationssicherheit**

- Richtiger Umgang mit Arbeitsmitteln (bspw. Emails, Kalender etc.)

03

Status Implementierung  
Zürcher Spitäler –  
2022 und heute

# Status Implementierung Zürcher Spitäler

## Entwicklung 2022 - heute

### 2022

- Unklarheiten bzgl. Umsetzung der regulatorischen Anforderungen
- Stand der Umsetzung der ISO 27001 bei ca. 35-40%
- Awareness beim Personal eher weniger gut bzgl. Security

### Heute

- Projektanforderungen klarer definiert
  - TOP Massnahmen zur Umsetzung definiert
- Umsetzung des Leitfadens und damit 50 – 60% der Anforderungen der ISO27001 umgesetzt
- Zahlreiche Awareness Kampagnen durchgeführt; Personal bzgl. Datenschutz und Security bereit.



04

# Cyberversicherungen und Standards (ISO27K & BSI)

# Cyberversicherungen und Standards

Einhaltung von Standards wird/ist Voraussetzung für Abschluss von Cyberversicherungen

## Versicherungskontext

- Steigende Risiken wegen
  - Steigender Anzahl und Schadenshöhe von Cyberangriffen
- Steigende Prämien
- Steigende Ablehnungsrate bei Kunden

## Leistungen von Versicherungen

- Finanzielle Schadensregulation
- Prävention
  - Vergünstigungen bei Dienstleistern
    - Penetration Tests
    - Zertifizierungsaudits
    - Analysesoftwarelizenzen
    - Awarenesstrainings
    - etc.
- Assistenz bei Vorfällen
  - Verhandlungsführer bei Ransomware
  - Forensiker für die Feststellung des aktuellen Schadensumfangs und der weiteren Vorgehensweise
  - etc.

## Zertifizierungen

- ISO27001
- B3S Standard für Krankenhäuser des deutschen BSI



05

Vorgehen bei x-tention

# Vorgehen x-tention

Auf Betriebsorganisation abgestimmte strukturierte Verknüpfung von Ist-Zustand, Standards & Erfahrungswerten

## Ist-Zustand

- Jedes Spital hat etwas im Bereich Datenschutz und Informationssicherheit.
  - IST-Analyse (zeigt auch den Fortschritt -Vorher/Nachher- auf)
  - ISO27001 GAP Analyse manchmal vorhanden

## Awareness

- **Geschäftsleitung:** Workshop zu Verantwortung bei Datenschutz, Informationssicherheit und Berufsgeheimnis
- **Belegschaft:** Awareness Trainings zu Datenschutz, Informationssicherheit und Berufsgeheimnis

## Standards & „Stand der Technik“

- Bedarfsgerechte Auswahl des anzuwendenden Standards
  - ISO27001
  - B3S Standard für Krankenhäuser
  - VZK Standard

## Erfahrungswerte

- Shared CISO, Shared DSB; ISMS + DSMS Implementation Beratung
- Vorlagenpakete speziell für Schweizer Krankenhäuser zu Datenschutz und Informationssicherheit, leicht anzupassen
  - Handelnde Personen (*Rolle, Aufgaben, Kompetenzen, Verantwortung*)
  - Benutzerrichtlinie, Datenschutzrichtlinie, Informationssicherheitsrichtlinie und Informationssicherheitsrichtlinie für Externe, Kennwortrichtlinie, Datenklassifizierungsrichtlinie, Zutrittskontrollrichtlinie, Zugriffskontrollrichtlinie, Kryptographie-Richtlinie, Richtlinie Softwaretests und Freigaben, Mobilgeräte richtlinie, Social-Media-Richtlinie etc.
  - Bearbeitungsverzeichnis, Datenschutz-Folgenabschätzung
  - IT-Notfallkonzept, Schulungskonzept
  - Informationssicherheits-Risikomanagement
  - ISMS-Massnahmenplan, DSMS-Massnahmenplan
  - Auditprogramm, Prozessbeschreibung Auditplanung
  - Prozessbeschreibungen Betroffenenrechte, Einwilligung & Widerruf, Active Directory, Anti-Malware, Asset-Management, Backup & Recovery, Berechtigungsvergabe, Notfallmanagement, Change Management, Monitoring, Patch Management, Security Incident Management etc.
  - etc.

06

# „Stand der Technik“ als Rechtsbegriff

Schutzmassnahmen zur Minimierung der Haftung



# Rechtsbegriff „Stand der Technik“

Beispiele praktischer Anwendungsfälle / Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit

## «Stand der Technik» ist ein Rechtsbegriff für Vorgehensweisen & Technologieanwendung

*(In der Informationstechnologie sind die Entwicklungszyklen zu kurz, um in Gesetzen Technologieanwendung festzuschreiben. Es gibt daher auch kein Gesetz, das den Technologieeinsatz spezifiziert. I.d.R. verweisen Gesetze auf den «Stand der Technik».)*

- Die Rechtsprechung legt «Stand der Technik» meist anhand der ISO 14971:2019 aus, als  
„entwickeltes Stadium der **technischen Möglichkeiten** zu einem bestimmten Zeitpunkt ... basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung“  
und ergänzt mit dem Hinweis  
„Stand der Technik“ umfasst die gegenwärtig und allgemein anerkannte gute Praxis bei Technologie und Medizin. ... bedeutet nicht unbedingt die technisch fortgeschrittenste Lösung.
- Die GDK und der Kanton Zürich orientieren den «Stand der Technik» für ISMS an den einschlägigen internationalen Standards
  - ISO 2700x-Reihe
  - Vorgaben des deutschen Bundesamtes für Sicherheit in der Informationstechnik BSI)

Ermittlung von qualitativen Kriterien anhand der 3-Stufen-Theorie - beginnend mit Geringwertigen:

- **„(allgemein) anerkannte Regeln der Technik“:**  
„wissenschaftlich anerkannt“ und „praktisch bewährt“; von Privaten verabschiedete technische Normen, wie bspw. DIN, ISO, ITIL® (Axelos), TOGAF® (Open Group), MSA (Microsoft), MOF (Microsoft) etc.
- **„Stand der Technik“:** „wissenschaftlich anerkannt“; höherwertig als „(allgemein) anerkannte Regeln der Technik“, aber noch nicht aktuelle wissenschaftliche Fachdiskussion. (Ältere wissenschaftliche Fachdiskussion kann nach gewisser Zeit zum «Stand der Technik» werden.)
- **„Stand von Wissenschaft und Technik“:** Das, worüber in Forschung, Publikationen und wissenschaftlicher Fachdiskussion Konsens besteht.

07

Dos & Don'ts

# Dos & Don'ts

## Dos

- **Datenschutz und Informationssicherheit leben**
- Ist-Analyse vor Projekt und dann jährlich
- Priorisiert anhand der Ist-Analyse vorgehen
- Abgestimmt auf verfügbare Ressourcen planen
- Geschäftsleitung aktiv einbeziehen und fordern
- Risikoträger und Eigentümer (Geschäftsleitung) klar deklarieren, dort Entscheidungen einholen
- Laufend Awareness schaffen und halten
- Botschafter für Datenschutz und Informationssicherheit in der gesamten Organisation definieren und aktiv einbeziehen

## Don'ts

- Datenschutz, Informationssicherheit nur als Projekt
- Einfach einmal anfangen
- Alles auf einmal anfangen
- Übersteuern der täglichen Aufgaben durch Projekt
- Geschäftsleitungsaussagen einfach folgen
- Risikozuweisung ausserhalb der Geschäftsführung akzeptieren
- Belegschaftsschulungen & Trainings > 30 Minuten
- Auf „Datenschutz verbietet“ oder „Informationssicherheit verbietet“ ohne weitere Begründung hören.

# Hier finden Sie weitere Informationen:



[x-tention.com/schweiz](https://x-tention.com/schweiz)



[healthcare-security.ch](https://healthcare-security.ch)



[x-tention.com/  
informationssicherheit-  
und-datenschutz](https://x-tention.com/informationssicherheit-und-datenschutz)



[x-tention.com/  
informationssicherheits-und-  
datenschutz-managementsystem](https://x-tention.com/informationssicherheits-und-datenschutz-managementsystem)

# Vielen Dank für Ihr Interesse!

## **Hellmuth Brandt**

Telefon: +41 43 500 26 37

E-Mail: [hellmuth.brandt@x-tention.com](mailto:hellmuth.brandt@x-tention.com)

x-tention Informationstechnologie AG

Bellerivestrasse 3

8008 Zürich

Schweiz

## **Andre Baumgart**

Telefon: +41 44 943 16 63

E-Mail: [baumgart@vzk.ch](mailto:baumgart@vzk.ch)

Verband Zürcher Krankenhäuser

Nordstrasse 15

8006 Zürich

Schweiz