

# TeleTrust-Informationstag "IT-Sicherheit in der ärztlichen Praxis"

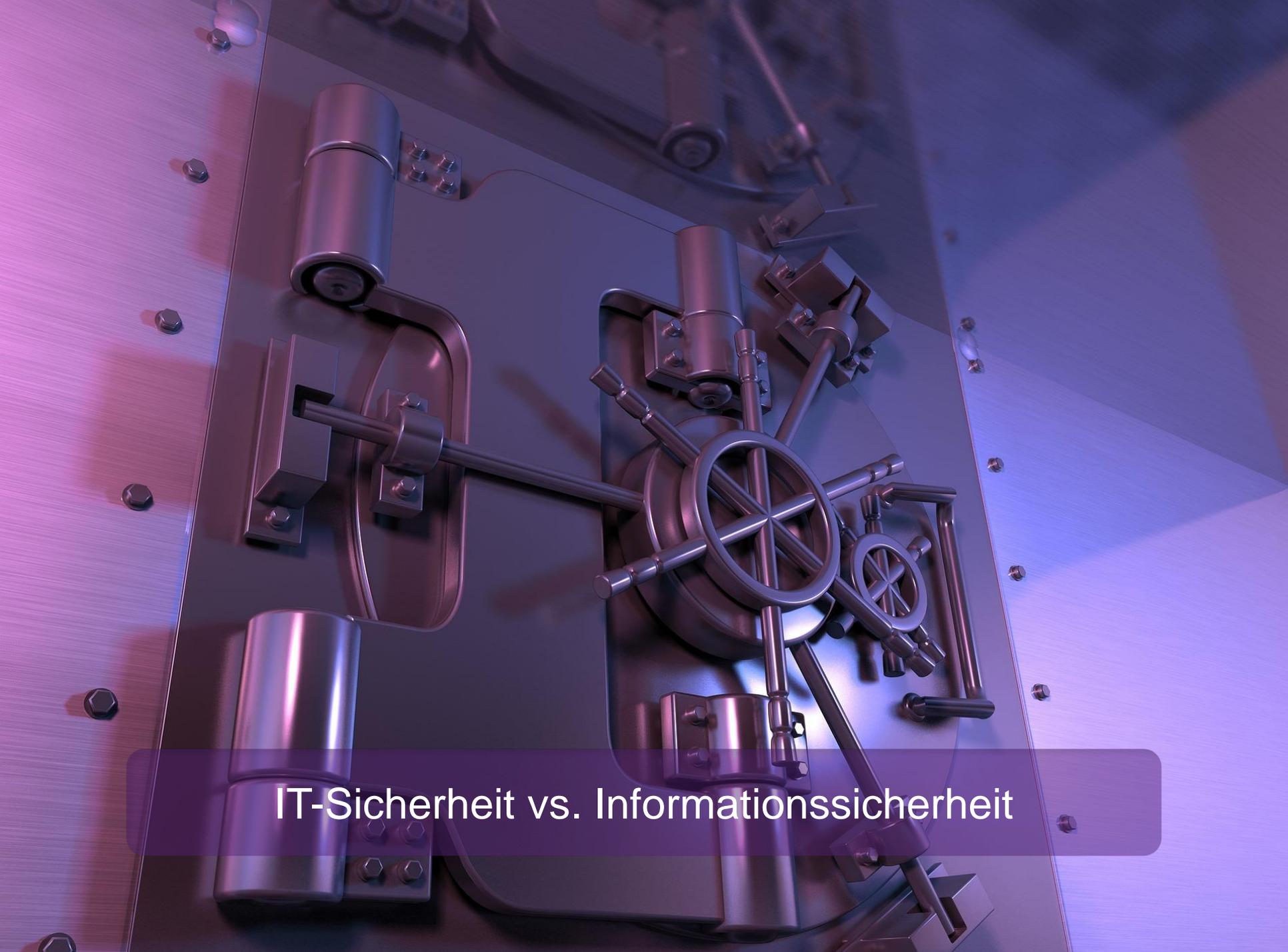
Berlin, 31.05.2017

## Rolle der Körperschaften und Aktivitäten der KBV

Heinz-Theo Rey, KBV

# Agenda

1. IT-SICHERHEIT VS. INFORMATIONSSICHERHEIT
2. INFORMATIONSSICHERHEIT BEI DER KBV
3. INFORMATIONSSICHERHEIT BEI KASSENÄRZTLICHEN VEREINIGUNGEN
4. INFORMATIONSSICHERHEIT FÜR DIE ARZTPRAXIS AUS SICHT DER KBV / KVEN
5. NÄCHSTE SCHRITTE



IT-Sicherheit vs. Informationssicherheit

## IT-Sicherheit vs. Informationssicherheit

IT-Sicherheit	Informationssicherheit
Geräte und Betriebsmittel, Systeme	IT-Sicherheit
Firewall, Virens Scanner, sichere Anwendungen	Gebäudesicherheit, Sicherheitsbereiche, Personalsicherheit
Backup-Konzept, Archivierung	Informationsklassifizierung, -kennzeichnung ( <u>Papier</u> )
Zugriffssteuerung, Zugangssteuerung	Sicherheitsorganisation, -überwachung
Netzwerkmanagement, Redundanzen	Lieferantensteuerung
IT-Prozesse und Organisation	Meldewege, Compliance, Audits, Business Continuity Management



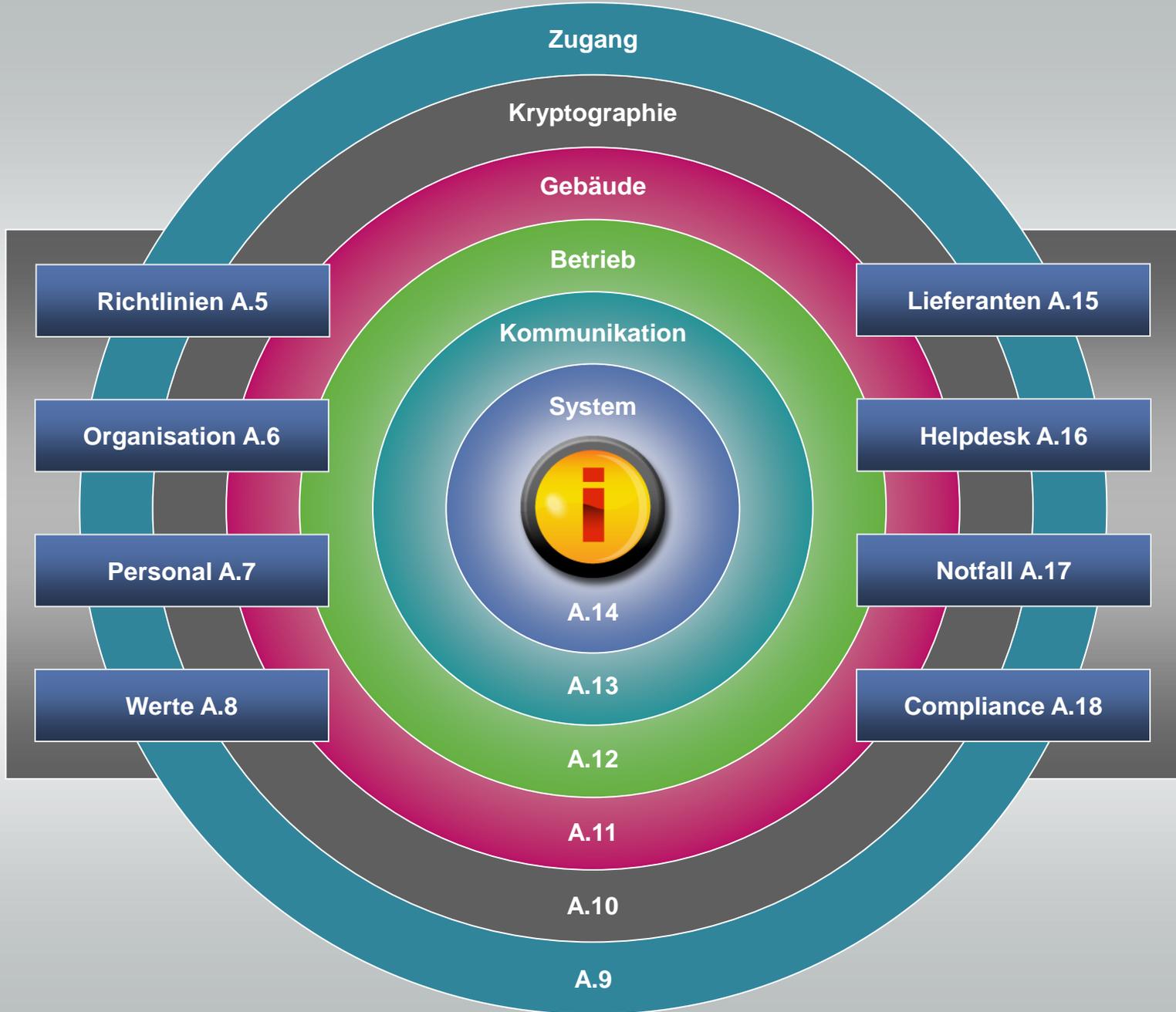
Information Security Management System

ISO

27001

Certified

Controls der ISO 27001, Anhang A





Status KBV

# ZERTIFIKAT

TÜV NORD

TÜV NORD

für das Managementsystem nach  
**ISO/IEC 27001:2005**

Der Nachweis der regelwerkskonformen Anwendung wurde erbracht und wird gemäß  
TÜV NORD CERT-Verfahren bescheinigt für



**Kassenärztliche Bundesvereinigung**  
Herbert-Lewin-Platz 2  
10623 Berlin  
Deutschland

# ZERTIFIKAT

für das Managementsystem nach  
**ISO/IEC 27001 : 2013**

Der Nachweis der regelwerkskonformen Anwendung wurde erbracht und wird gemäß  
TÜV NORD CERT-Verfahren bescheinigt für

**Kassenärztliche Bundesvereinigung**  
Herbert Lewin Platz 2  
10623 Berlin  
Deutschland



Geltungsbereich

**Analyse und Recherche von Gesundheitsdaten und -organisationen auf der  
Grundlage der fall- und vorgangsbezogenen Leistungsdaten**

**Unter Berücksichtigung der Erklärung zur Anwendbarkeit Version 1.10 vom 15.11.2016.**

Zertifikat-Registrier-Nr. 44 121 101834  
Auditbericht-Nr. 3518 5680

Gültig bis 2019-12-18  
Erstzertifizierung 2010

  
Zertifizierungsstelle  
der TÜV NORD CERT GmbH

Essen, 2017-01-31

Diese Zertifizierung wurde gemäß TÜV NORD CERT-Verfahren zur Auditierung und Zertifizierung durchgeführt und wird  
regelmäßig überwacht.

TÜV NORD CERT GmbH

Langemarckstraße 20

45141 Essen

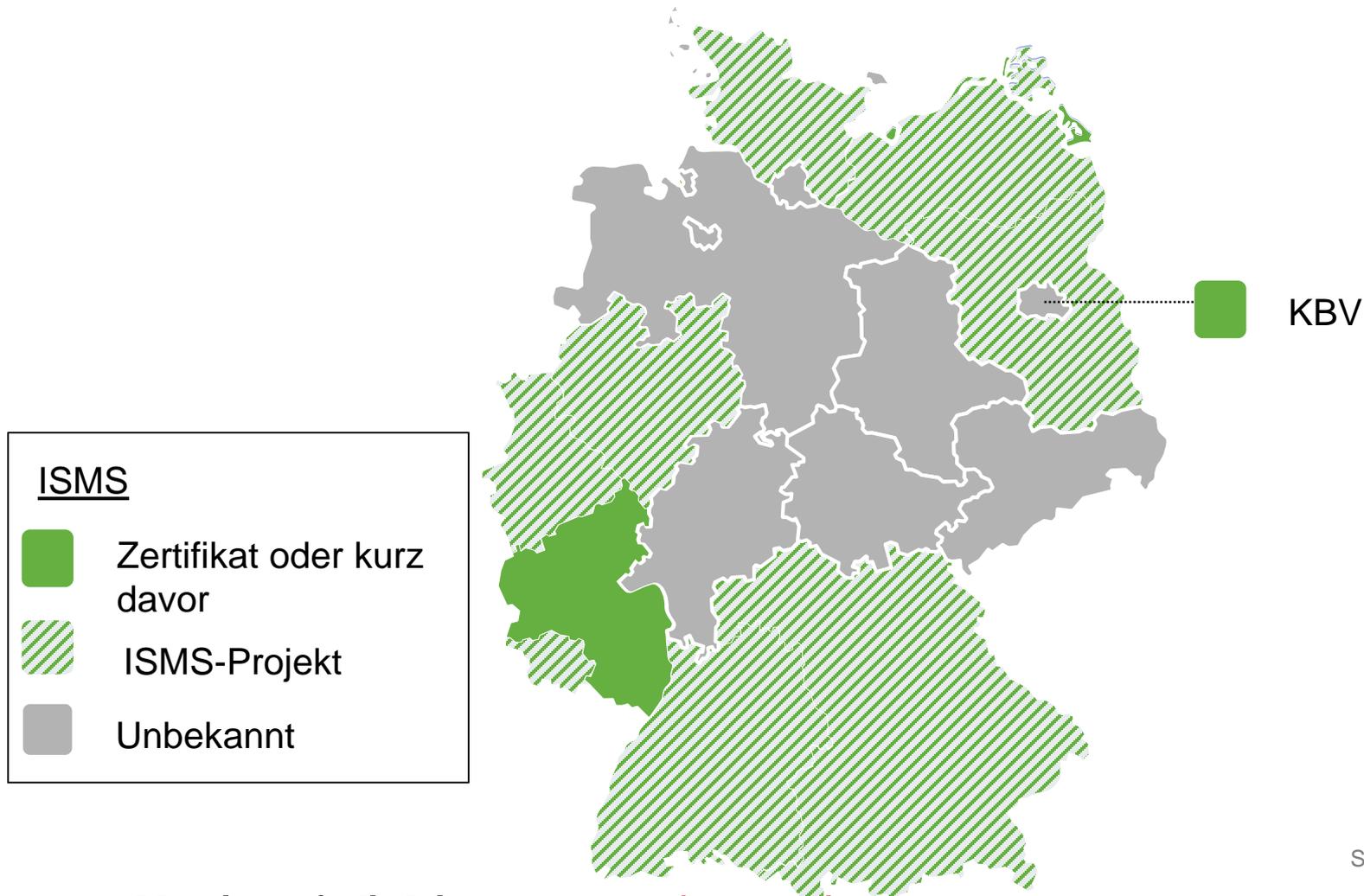
[www.tuev-nord-cert.de](http://www.tuev-nord-cert.de)



A photograph of a modern, multi-story glass building at night. The building's interior lights are on, and the sky is a deep blue. A semi-transparent grey box is overlaid at the bottom of the image, containing the text "Status Kassenärztliche Vereinigungen".

Status Kassenärztliche Vereinigungen

# ISMS bei den Kassenärztlichen Vereinigungen



Stand 16.09.2016



Arztpraxen

# Arztpraxis: Maßnahmen der KBV

## BEKANNTGABEN DER HERAUSGEBER

BUNDESÄRZTEKAMMER

KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

## Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis<sup>1</sup>

### 1. Einleitung

Die ärztliche Schweigepflicht ist von grundlegender Bedeutung für das besondere Vertrauensverhältnis zwischen Arzt und Patient<sup>2</sup>. Ärzte haben über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen. Die ärztliche Schweigepflicht zählt zum Kernbereich der ärztlichen Berufsethik. Die rechtliche Ausgestaltung der Schweigepflicht erfolgt durch die Bestimmungen des § 9 Abs. 1 der (Muster-)Berufsordnung der in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) sowie die entsprechenden Regelungen der Berufsordnungen der Landesärztekammern<sup>3</sup>.

Neben dem Vertrauensverhältnis zwischen Arzt und Patient umfasst der Schutzzweck der ärztlichen Schweigepflicht auch die Wahrung des Patientengeheimnisses, dessen Verletzung durch den Arzt mit Geld- oder Freiheitsstrafe geahndet werden kann.

Bei der elektronischen Datenverarbeitung in der Arztpraxis ist ebenfalls das Recht auf informationelle Selbstbestimmung des Patienten zu beachten. Für die niedergelassenen Ärzte sind insbe-

sondere das StGB geschützte Patientengeheimnis, das entsprechende Verstöße des Arztes gegen die Verschwiegenheitspflicht strafrechtlich sanktioniert. Nach § 203 Abs. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm als Arzt anvertraut worden oder sonst bekanntgeworden ist. Ein Verstoß gegen die ärztliche Schweigepflicht kann daher neben berufsrechtlichen oder berufsgerichtlichen Maßnahmen auch Schadensersatzansprüche und sogar strafrechtliche Konsequenzen zur Folge haben.

### 2.2 Reichweite

Die ärztliche Schweigepflicht umfasst alle Tatsachen, die nur einem bestimmten, abgrenzbaren Personenkreis bekannt sind und an deren Geheimhaltung der Patient ein verständliches, also sachlich begründetes und damit schutzwürdiges Interesse hat. Sie ist grundsätzlich auch gegenüber anderen Ärzten, Familienangehörigen des Patienten sowie eigenen Familienangehörigen

# Empfehlungen zur ärztl. Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

- Allgemeine Organisatorische Regelungen
- Technische Anlage
  - Passwörter
  - Schutz gegen Schadsoftware
  - Begrenzung von Privilegien
  - Nutzung von Intranet und Internet
  - LAN, WLAN
  - Verschlüsselung, Backup, Entsorgung von Geräten und Datenträgern
  - Einspielen von Sicherheitsupdates
  - Fernwartung
  - Elektronische Dokumentation und Archivierung
- Addendum: Elektronische Kommunikation, Backup, digitale Signatur, ersetzendes Scannen Powerline, Kryptograie, VoIP, DECT-Telefonie, externe Dienstleister zur Archivierung von ärztl. Dokumentation

## Arztpraxis: Maßnahmen der KBV (Mein PraxisCheck)

### › Informationssicherheit

Sind sensible Patientendaten in Ihrer Praxis sicher? Wie sind die Zugriffsrechte auf das EDV-System geregelt? Wie wird die Stromversorgung Ihres Datenservers gewährleistet? Überprüfen Sie hier die Informationssicherheit Ihrer Praxis – und sehen Sie, was noch verbessert werden kann.



# Arztpraxis: Maßnahmen der KBV (Mein PraxisCheck)

Frage 1 von 19

[Check abbrechen und Ergebnisse anzeigen](#)

**Wie stellen Sie bei der Erhebung der Patientendaten eine angemessene akustische Abschirmung sicher?**

Durch ausreichenden Abstand zu anderen Patienten bzw. günstige räumliche Gegebenheiten sowie sensible und geschulte Mitarbeiter sind uns eine diskrete Datenerhebung und Kommunikation möglich.

Wir bemühen uns um eine diskrete Datenerhebung und Kommunikation, jedoch sind die räumlichen Gegebenheiten ungünstig.

Bislang gab es keine Beschwerden wegen fehlender akustischer Abschirmung.

Weiß nicht.

Jeder Patient hat ein Recht auf Schutz der Intimsphäre. Hilfreich für eine diskrete Datenerhebung und Kommunikation sind bspw. eine separate Anmeldung, Trennwände, Hintergrundmusik.

[Zurück](#)[Weiter](#)

# Arztpraxis: Maßnahmen der KBV (Mein PraxisCheck)

Frage 13 von 19

[Check abbrechen und Ergebnisse anzeigen](#)

**Wie stellen Sie sicher, dass Mitarbeiter und externe Dienstleister über die Vorgaben zu Schweigepflicht und Datenschutz informiert sind und diese einhalten?**

**Liegt von allen Mitarbeitern und externen Dienstleistern eine unterschriebene Datenschutzerklärung vor?**

Alle Mitarbeiter und externen Dienstleister haben eine Datenschutzerklärung unterschrieben und erfüllen die Vorgaben zu Schweigepflicht und Datenschutz. Die Leitung hat eine/n Datenschutzbeauftragte/n schriftlich festgelegt (erforderlich bei mehr als neun Personen, die ständig mit der automatischen Verarbeitung von personenbezogenen Daten beschäftigt sind).

Die Mitarbeiter haben teilweise eine Datenschutzerklärung unterschrieben und versuchen die Vorgaben zur Schweigepflicht und zum Datenschutz zu erfüllen.

Wir wissen, dass es Vorgaben zu Schweigepflicht und Datenschutz gibt und glauben, diese "aus dem Bauch heraus" zu erfüllen.

Weiß nicht.

Holen Sie systematisch von allen Mitarbeitern (auch von Praktikanten) und externen Dienstleistern (z. B. EDV-Berater/Support-Mitarbeiter und Reinigungspersonal) Datenschutzerklärungen ein. Weisen Sie nicht nur bei der Einstellung neuer Mitarbeiter auf die Vorgaben hin, nutzen Sie dazu auch die regelmäßigen Teamsitzungen und Mitarbeitergespräche. Bei mehr als neun festangestellten Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, muss die Leitung eine/n Datenschutzbeauftragte/n festlegen.

[Zurück](#)[Weiter](#)

# Arztpraxis: Maßnahmen der KBV (Mein PraxisCheck)

Frage 16 von 19

Check abbrechen und Ergebnisse anzeigen

## Wie erfolgt die Sicherung der Daten?

Die Sicherungen erfolgen nach dem Drei-Generationen-Prinzip am Abend eines Praxistages, am Ende einer Woche und am Ende eines Monats. Dabei werden alle Rechner, auch die Laptops, berücksichtigt. Alle persönlichen Gesundheitsdaten werden in verschlüsselter Form gesichert.

Die Sicherungen erfolgen am Ende einer Woche und werden vier Wochen aufbewahrt. Danach werden die Sicherungsbänder erneut verwendet.

Es wird lediglich die Datenbank gesichert. Die aber täglich.

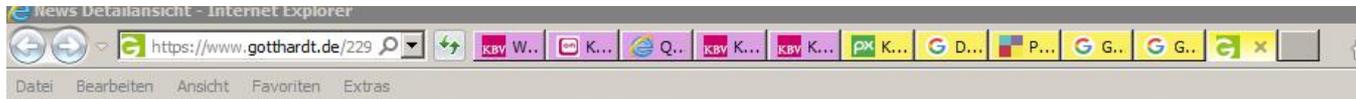
Weiß nicht.

**Achtung!** Wenn lediglich die Datenbank gesichert wird, also die Anwendungsdaten, können im Schadensfall die Software und die Systemdaten nicht mehr rekonstruiert werden. Alle Systeme müssten aufwendig neu installiert und konfiguriert werden, bevor die Anwendungsdaten wieder genutzt werden könnten.

[Zurück](#)[Weiter](#)

## Arztpraxis: Maßnahmen der KBV (Mein PraxisCheck)





Bundesgesetzblatt Jahrgang 2013 Teil I Nr. 9, ausgegeben zu Bonn am 25. Februar 2013

277

## Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten

Vom 20. Februar 2013

Der Bundestag hat das folgende Gesetz beschlossen:

hältnis im Sinne des § 622 ist, anzuwenden, soweit nicht in diesem Untertitel etwas anderes bestimmt ist.

### Artikel 1 Änderung des Bürgerlichen Gesetzbuchs

Das Bürgerliche Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 3 des Gesetzes vom 20. Februar 2013 (BGBl. I S. 273) geändert worden ist, wird wie folgt geändert:

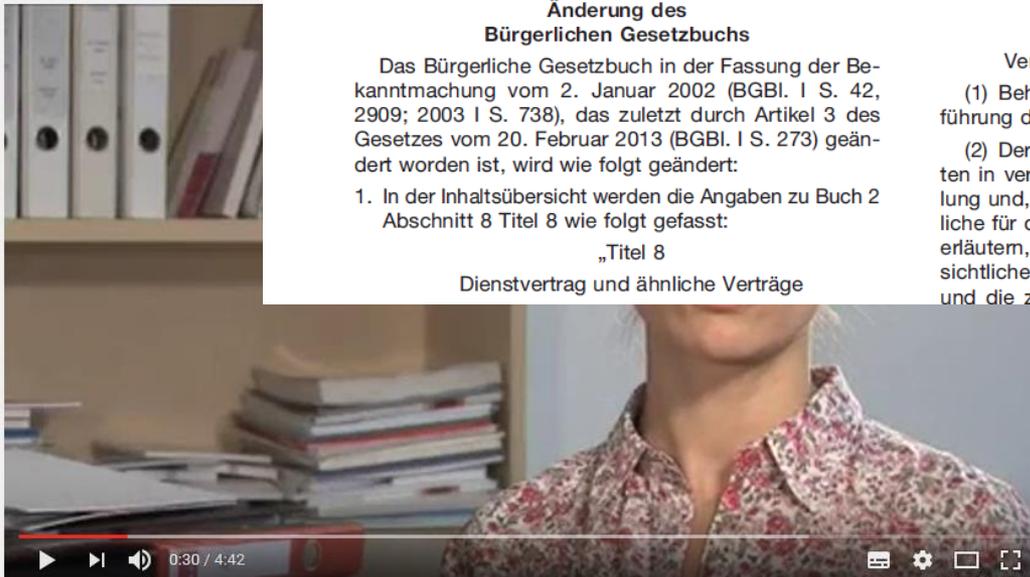
### § 630c Mitwirkung der Vertragsparteien; Informationspflichten

1. In der Inhaltsübersicht werden die Angaben zu Buch 2 Abschnitt 8 Titel 8 wie folgt gefasst:

(1) Behandelnder und Patient sollen zur Durchführung der Behandlung zusammenwirken.

(2) Der Behandelnde ist verpflichtet, dem Patienten in verständlicher Weise zu Beginn der Behandlung und, soweit erforderlich, in deren Verlauf sämtliche für die Behandlung wesentlichen Umstände zu erläutern, insbesondere die Diagnose, die voraussichtliche gesundheitliche Entwicklung, die Therapie und die zu und nach der Therapie zu ererfendenden

„Titel 8  
Dienstvertrag und ähnliche Verträge



Datenschutz in der Praxis

K VonTV  
Abonnieren 44



Suchen

Wähle deine Sprache aus.

Du siehst YouTube auf Deutsch.

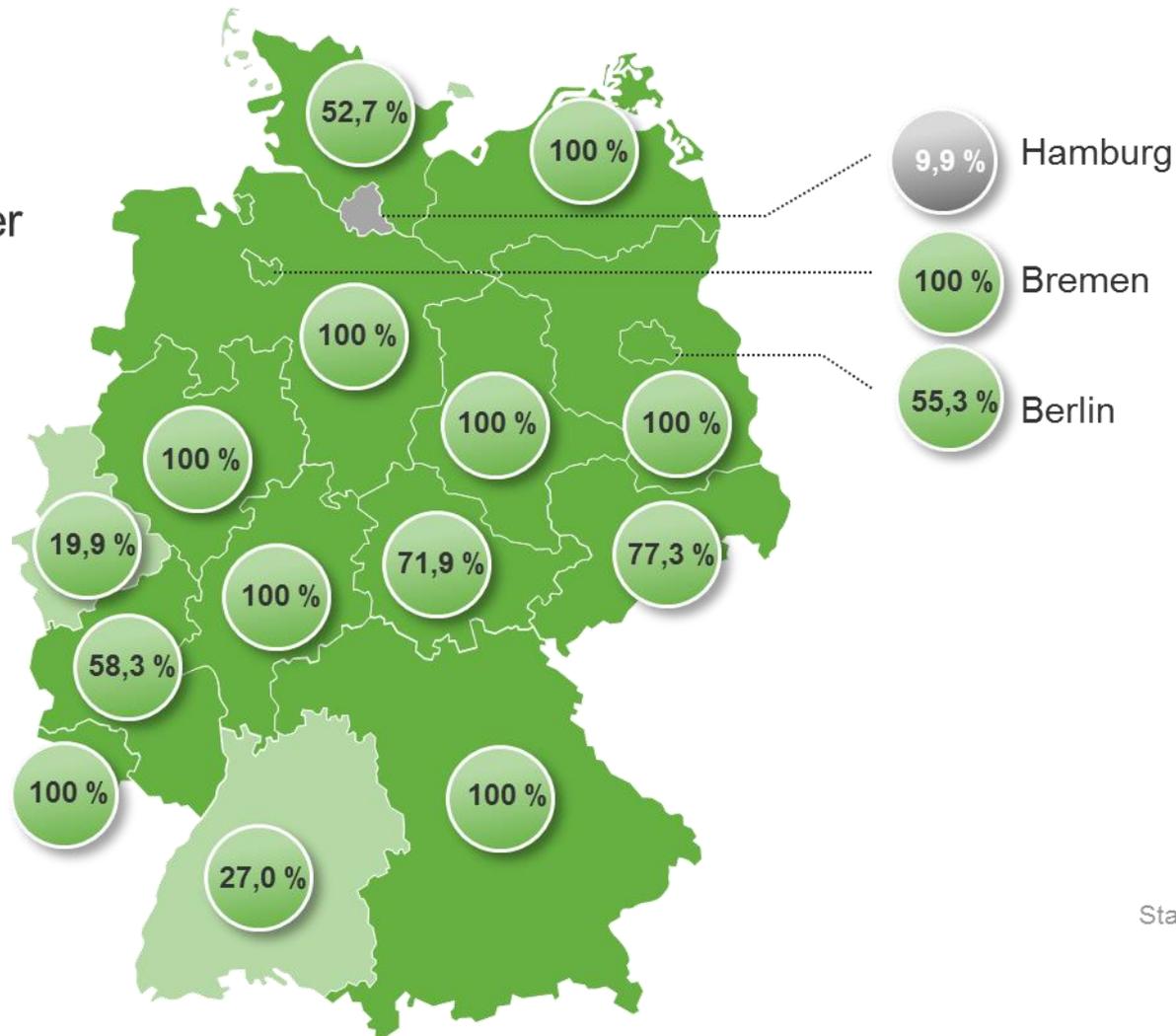
ks (87)

rt

Suche

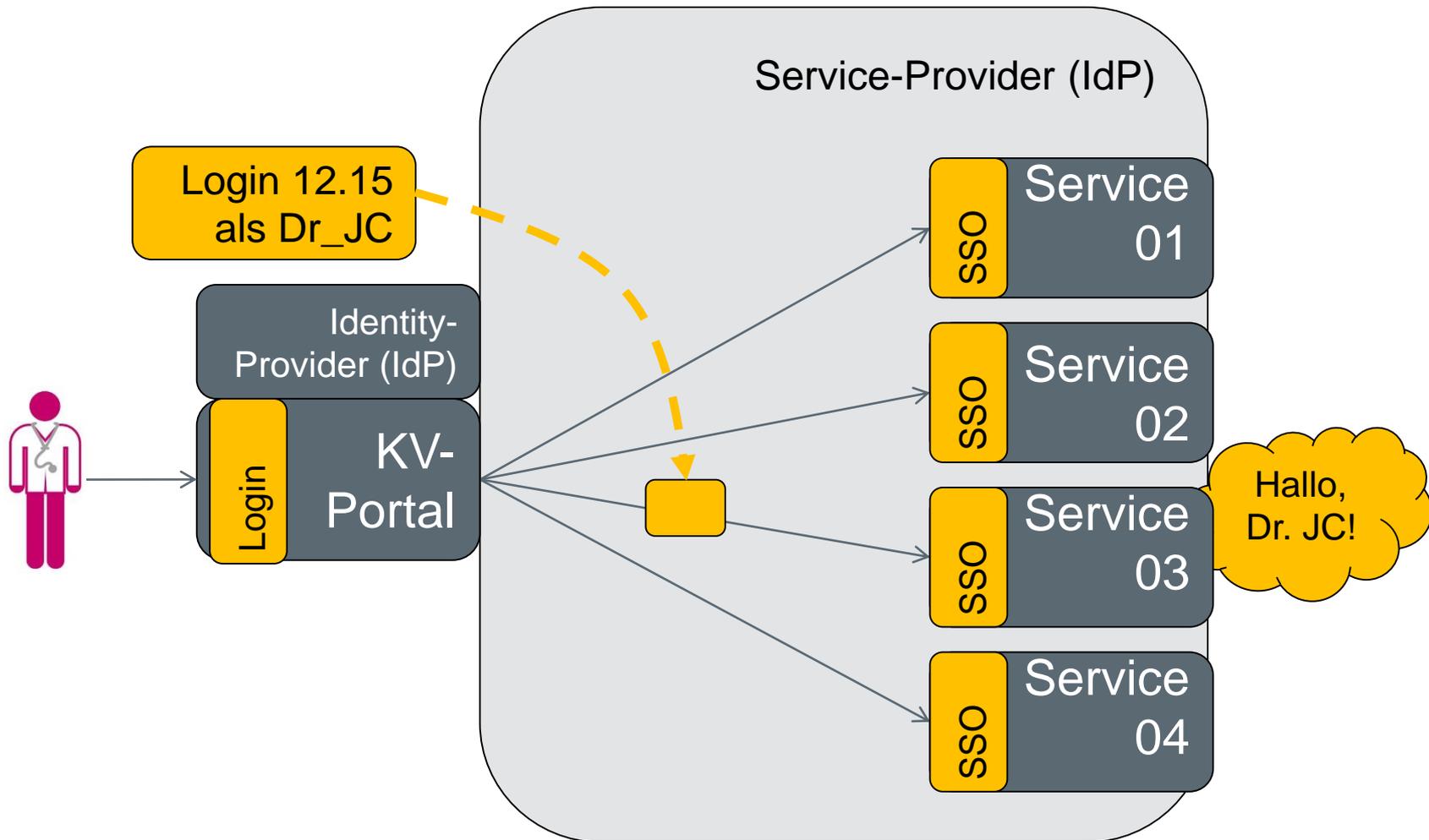
## Arztpraxis: Maßnahmen der KBV (KV-SafeNet)

Ca.:  
116.000 Teilnehmer



Stand 06.04.2017

## Arztpraxis: Maßnahmen der KBV (FIM)



SSO: Single sign on

## Digitale Arzt-Identität bei der KV

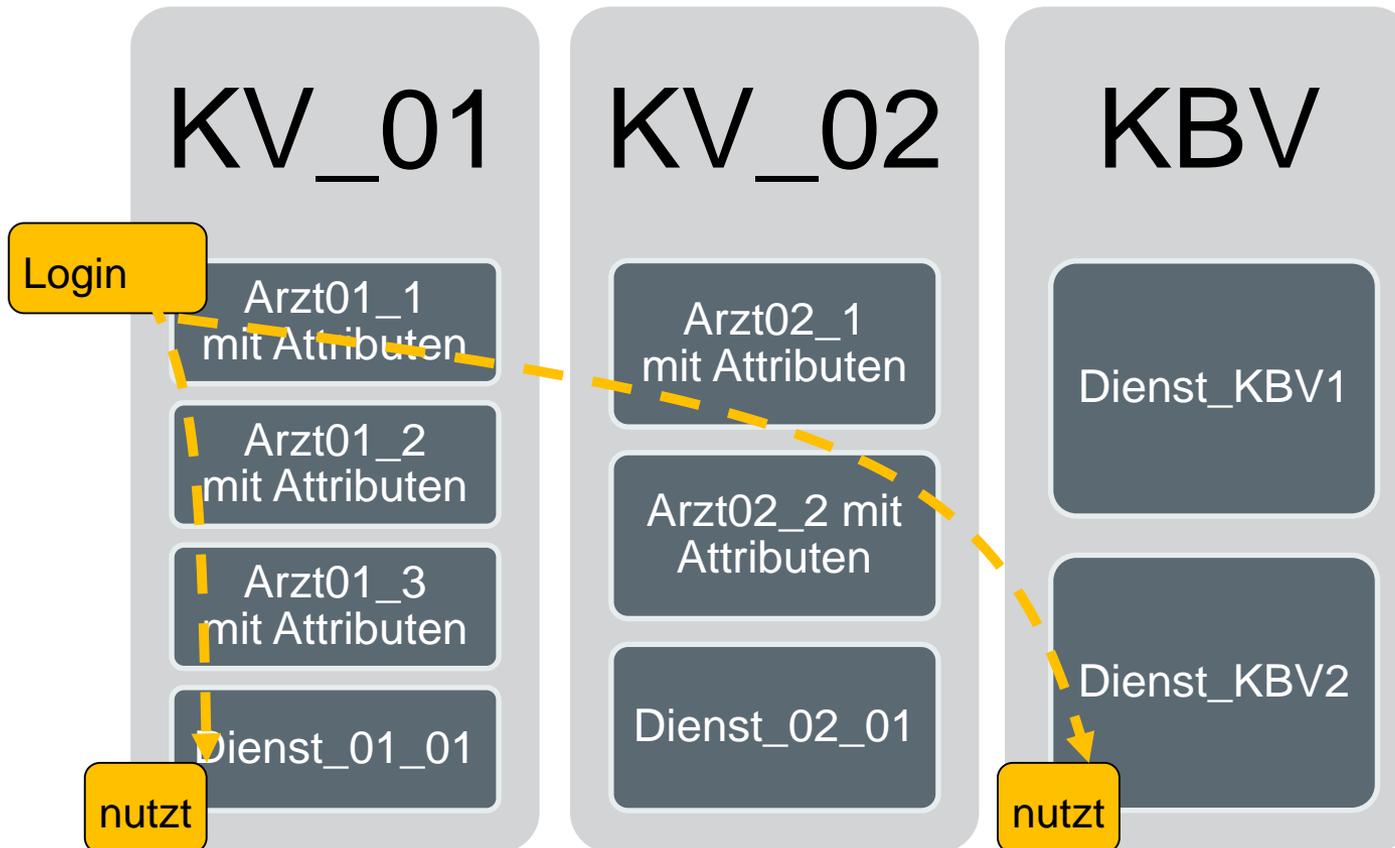
- Zulassung
- Arztgruppe
- LANR
- BSNR
- Genehmigungen
- Arzthelferinnen
- Wechsel BSNR
  
- Benutzername
- Passwort
- Passwort ändern
- Ende Zulassung

In einem föderierten System ist auch nur eine dezentrale **Pflege** der Daten möglich!

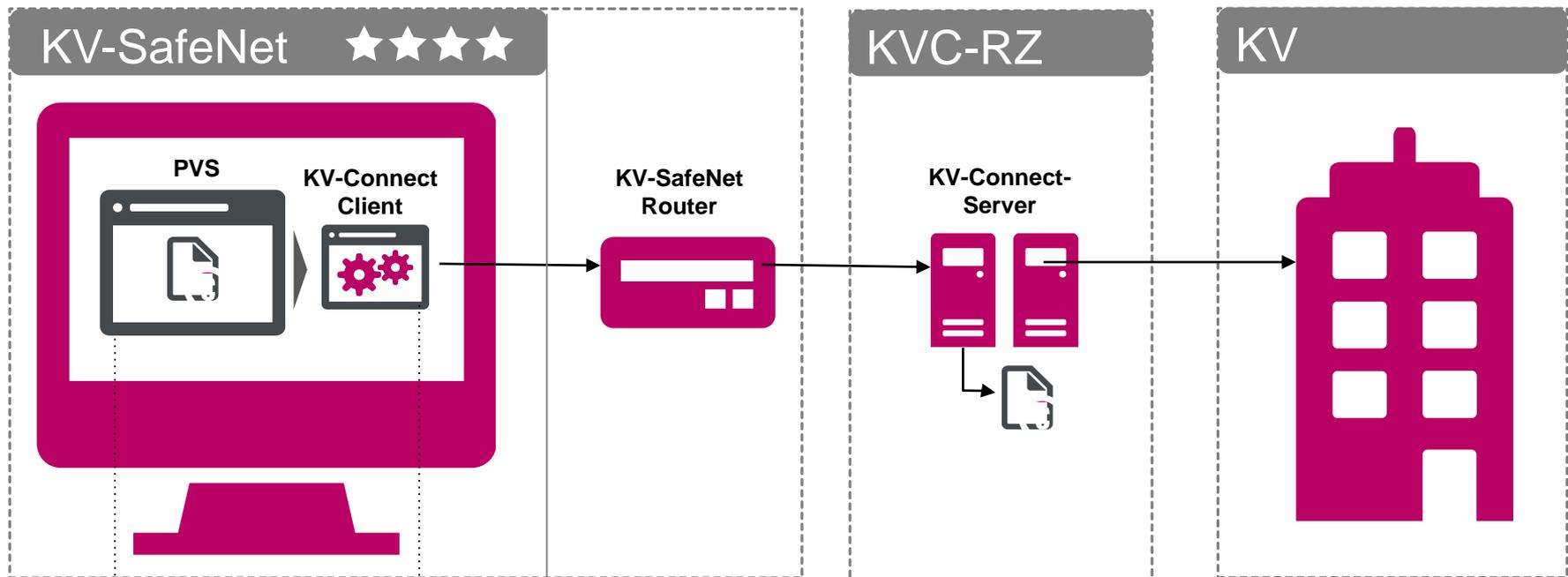
Zentrale  
Daten-  
haltung

**FIM!**

## Digitale Identität – gefördert!



## Arztpraxis: Maßnahmen der KBV (KV-Connect)



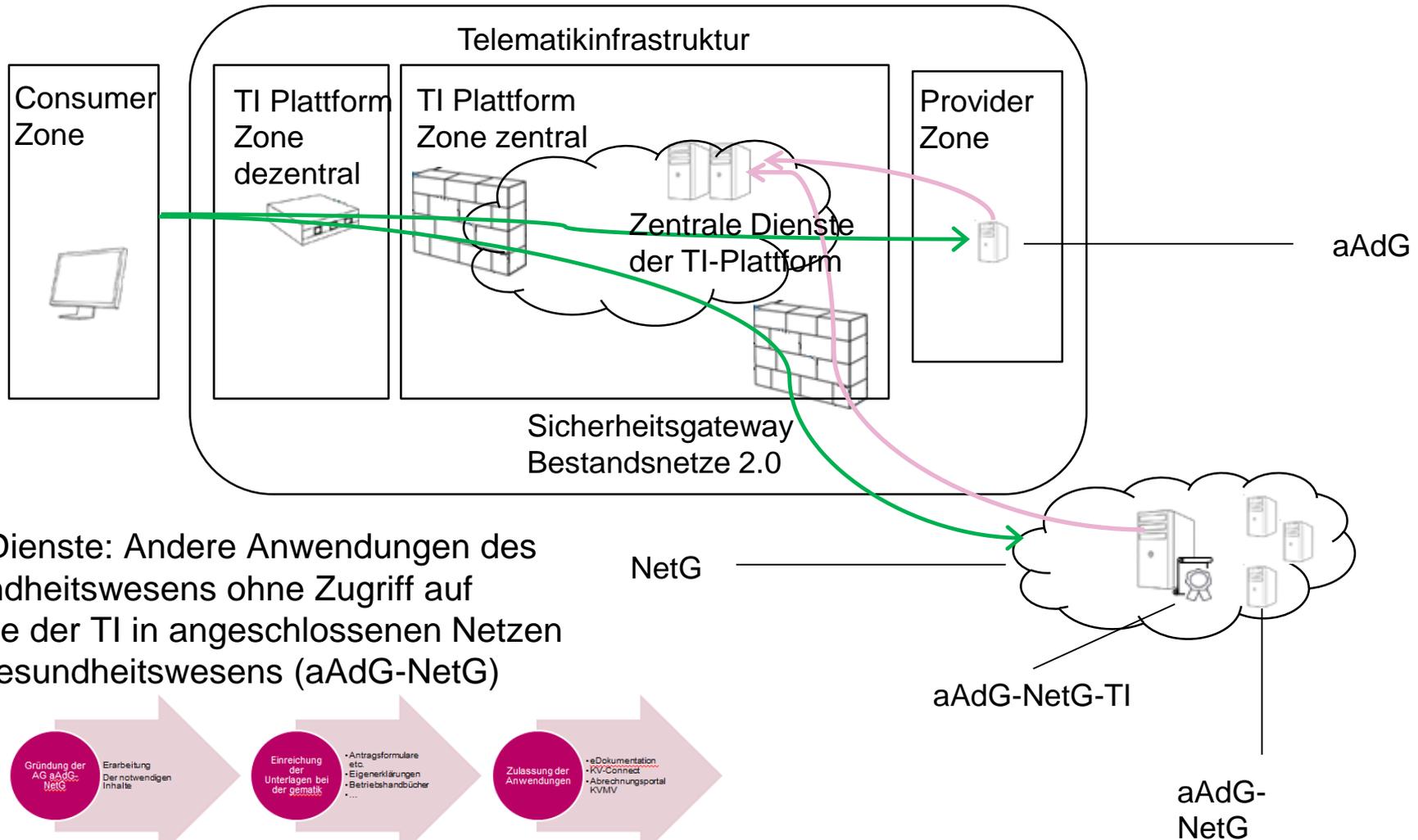
1a) Die Nachricht wird im PVS erstellt, geprüft und mit einem Click an den KV-Connect-Server übermittelt.

1b) Zur Übermittlung übergibt das PVS die Nachricht an den KV-Connect-Client (Software). Dieser übernimmt die Adressierung und verschlüsselte Übertragung.

2) Der KV-Connect-Server speichert die verschlüsselte Nachricht.

3) Der Empfänger (hier eine KV) entschlüsselt die Nachricht. Sie wird vom KV-Connect-Server gelöscht.

# Arztpraxis: Anbindung an die TI, Nutzung des SNK



## Echo auf die Maßnahmen der KBV

- "Da machen wir ein Modul draus. Ich liebe Module, die kann man so gut verkaufen..."

STATEMENT - BERLIN, 08.06.2016

### eGK/Telematik – Anwendungen in Parallelnetzen im Rahmen von Selektivverträgen

#### Erklärung des Verwaltungsrates des GKV-Spitzenverbandes zur Telematik

Der Verwaltungsrat des GKV-Spitzenverbandes unterstützt trotz der erneuten, durch die Anbieter verursachten Verzögerungen bei der Lieferung wichtiger Hardwarekomponenten weiterhin die Telematikinfrastruktur (TI) als derzeit einzig sicheres Netz des deutschen Gesundheitswesens. Die Telematikinfrastruktur gewährleistet das für medizinische Daten notwendige, sehr hohe Sicherheitsniveau durch permanente Einbindung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Das kürzlich verabschiedete eHealth-Gesetz unterstreicht diese Bedeutung an diversen Stellen, insbesondere durch die Klarstellung, dass der elektronische Arztbrief zukünftig nur noch über Dienste der Telematikinfrastruktur versendet werden darf. Bis zur Verfügbarkeit der Telematikinfrastruktur werden allerdings die Nutzung und der Aufbau von potentiell unsicheren Parallelnetzen nicht unterbunden, sondern im Rahmen von Selektivverträgen teilweise sogar gefördert.



Ausblick

## Ausblick

- Anstrengungen zur Erhöhung der Informationssicherheit in der Arztpraxis müssen erhöht werden
- Aktuelles Set von Maßnahmen ist ein erster Schritt, reicht aber nicht aus
- Die KBV wird sich hier noch stärker einbringen

» Ich leg  
mich fest.  
**Ich lass mich  
nieder.**«

*Beatrice Ranft*  
Beatrice Ranft,  
MEDIZINSTUDENTIN



**Die Haus- und  
Fachärzte  
von morgen**

Wir arbeiten für Ihr Leben gern.

[www.lass-dich-nieder.de](http://www.lass-dich-nieder.de)

» Wir arbeiten für Ihr Leben gern.« [www.ihre-aerzte.de](http://www.ihre-aerzte.de)