INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

# Erstellung von Informationssicherheits-konzepten für Kommunen nach Art. 11 Abs. 1 S. 2 BayEGovG

# Anpassung der Arbeitshilfe an die DSGVO

**Sascha Kuhrau**

Copyright © · All rights reserved.

# Unsere Themen heute

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

## Agenda

- **Aktuelle Entwicklungen**
  - Novellierung BayEGovG
  - Die EU Datenschutz-Grundverordnung (DSGVO)
- **Arbeitshilfe 2.0**
  - Kapitel 2 Datenschutz – mehr als ein Facelift
  - Weitere Anpassungen
- **Die Arbeitshilfe im praktischen Einsatz**
  - Berichte von Anwendern
  - Umsetzungsmöglichkeiten
  - Externe Unterstützung zwingend notwendig?
  - Software-Unterstützung
  - Zeitaufwand

Copyright © · All rights reserved.

# Aktuelle Entwicklungen - BayEGovG

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

## Novellierung BayEGovG

- Ursprüngliche Version vom 22.12.2015
- Änderung durch § 1 des Gesetzes vom 27. November 2017 (GVBl. S. 518)
- Art.8 Informationssicherheit und Datenschutz geht auf in eigenem Teil
  - Teil 2 Sicherheit in der Informationstechnik
    - Art. 9+10 LSI und Aufgaben
    - Art. 11 Behördenübergreifende Pflichten:
    - *(1) Die Sicherheit der informationstechnischen Systeme der Behörden, die in den Anwendungsbereich des Teils 1 fallen, ist im Rahmen der Verhältnismäßigkeit sicherzustellen. Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn des Art. 7 des Bayerischen Datenschutzgesetzes (BayDSG) und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.*
    - *(2) Werden staatlichen oder sonstigen an das Behördennetz angeschlossenen Stellen Informationen bekannt, die zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind, unterrichten diese das Landesamt und ihre jeweilige oberste Dienstbehörde unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen.*
    - *Art. 19 Absatz 2 Art. 11 Abs. 1 Satz 2 tritt in Kraft am 01.01.2019*

Copyright © · All rights reserved.

# Aktuelle Entwicklungen - DSGVO

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

## ► Die EU Datenschutz-Grundverordnung (kurz DSGVO)

- Inkraftgetreten am 24.05.2016, somit
- Wirksam ab dem 25.05.2018 (2 Jahre Übergangsfrist bzw. Vorbereitungszeit)
- Grundverordnung ersetzt ausnahmslos nationales Recht in den EU Mitgliedsstaaten
- Öffnungsklauseln ermöglichen Ergänzungen / Verschärfungen in geringem Umfang auf nationaler Ebene durch sog. „Anpassungsgesetze“ / „Ausführungsgesetze“
- DSGVO Hauptrecht, nationale (Datenschutz-) Anpassungsgesetze Unterrecht
- BayDSG-E noch nicht verabschiedet
  - Kein Drama, denn die „big points“ sind in der DSGVO geregelt und daher auch ohne das „neue BayDSG“ umsetzbar
- Vorteile
  - Ein Recht für alle (EU Mitgliedsstaaten) / Harmonisierung
  - In weiten Teilen Angleichung des Datenschutzes für öffentliche und nicht-öffentliche Stellen
  - Viele Grundprinzipien des deutschen Datenschutz-Rechts eingeflossen

Copyright © · All rights reserved.

# Aktuelle Entwicklungen - DSGVO

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

## ► Die EU Datenschutz-Grundverordnung (kurz DSGVO)

- Probleme
  - Wegfall des bisher gut bekannten und auch durch Kommentare sowie Urteile unterstützten deutschen Datenschutz-Rechts
  - Fast alle Mitgliedsstaaten haben nationale Anpassungsgesetze erlassen, Deutschland 1 BDSG und 16 Landesdatenschutz-Anpassungen!!
  - Deutungshoheit auf EU Ebene
  - Gerade für neue Regelungen wenig bis keine Unterstützung durch Aufsichtsbehörden
    - Unterschiedliche Vorstellungen
    - Keine verbindlichen Aussagen, da EU Datenschutz-Kommission noch keine Auslegungen herausgegeben hat
    - Arbeitspapiere gelegentlich reine Wiederholung der Formulierungen aus der DSGVO
  - Kommentare in Überarbeitung bzw. Neufassung
    - „Erste Würfe“
    - Nur bedingt belastbar, da noch keine Erfahrungen mit der Anwendung der DSGVP

Copyright © · All rights reserved.

# Aktuelle Entwicklungen - DSGVO

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

## ► Die EU Datenschutz-Grundverordnung (kurz DSGVO)

- Teilweise: Alter Wein in neuen Schläuchen
  - Aus Verfahrensverzeichnis wird Verzeichnis der Verarbeitungstätigkeiten (erweiterte Angaben als bisher)
  - Aus Auftragsdatenverarbeitung (externe Dienstleister) wird Auftragsverarbeitung
  - Verfahrensfreigabe entfällt, dafür Datenschutz-Folgenabschätzung (DSFA)
  - Betonung der Aufgabenverteilung und Verantwortlichkeiten in der Organisation
  - Generelle Bestellpflicht eines Datenschutzbeauftragten (DSB) im öffentlichen Bereich (EU weit)
  - Mehrere Organisationen können sich einen DSB „teilen“
- Neu (Auszüge)
  - Informationspflichten gemäß Art. 13 und 14 DSGVO
  - Meldepflicht von Datenpannen für öffentliche Stellen
  - Öffentliche Bekanntgabe des Datenschutzbeauftragten auf Webseite sowie Meldung an den Landesdatenschutzbeauftragten
  - Externe Bestellmöglichkeit für Datenschutzbeauftragte mittels Dienstleistungsvertrag

Copyright © · All rights reserved.

# Aktuelle Entwicklungen - DSGVO

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

## ► Die EU Datenschutz-Grundverordnung (kurz DSGVO)

- DSGVO kommt nicht „überraschend“
- DSGVO kann bereits seit 23 Monaten aktiv bearbeitet / vorbereitet werden
- Keine Notwendigkeit, auf Vollständigkeit von Handreichungen und Vorlagen zu warten,
  - denn es gibt sehr viel zu tun.
  - bestehende Lücken müssen zeitnah geschlossen werden.
  - Transparenz- und Informationspflichten zeigen mangelnden Datenschutz klar und offen nach außen auf (jederzeit von außen durch Betroffene und Aufsichtsbehörden überprüfbar)
  - die Zeit drängt (25.05.2018 ist Stichtag).
- Übrigens: Datenschutz findet in der ganzen Organisation statt und ist nicht Aufgabe eines Einzelnen
  - Verantwortung für die Umsetzung (Bürgermeister, Landrat)
  - Delegiert Umsetzung an Fachbereichsleiter
  - DSB berät, überwacht und kontrolliert (Kontrollfunktion wurde erweitert)
  - Teilweise Delegationsmöglichkeit an DSB, jedoch beschränkt durch Vermeidung von Interessenskonflikten bei Überwachung und Kontrolle gesetzlich vorgeschrieben

Copyright © · All rights reserved.

# Fazit Aktuelle Entwicklungen

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Arbeitshilfe muss überarbeitet / aktualisiert werden**
  - Anpassungen an BayEGovG
  - Anpassungen an EU DSGVO
- **Gelegenheit zur weiteren Überarbeitung**
  - Umsetzungstipps aus der bisherigen Anwendung der Arbeitshilfe in der Praxis
  - Zusätzliche Vorlagen
  - Querverweise auf neuen BSI IT-Grundschutz Standard 200-2

Copyright © · All rights reserved.

# Bestandsaufnahme

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

## ► 9 Kapitel / Themenbereiche

- Informationssicherheit – Grundlagen zur Einführung und zur Aufrechterhaltung von Informationssicherheit
- **Datenschutz – Grundlegende Umsetzungen im Datenschutz (auf Basis der EU DSGVO) als elementarer Bestandteil der Informationssicherheit**
- Gebäudesicherheit
- Zugang zu IT-Systemen*
- Berechtigungskonzepte und Protokollierung*
- Notfallmanagement (Vorsorge und Notfallplan)*
- Richtlinien und Dienstanweisungen
- Schulungen und Sensibilisierung – Mitarbeiter als elementarer Bestandteil der Informationssicherheit
- Externe Dienstleister – Anforderungen an externe Dienstleister, nicht nur im Rahmen einer Auftragsdatenverarbeitung

* Klassische IT-Themen

Copyright © · All rights reserved.

# Arbeitshilfe 2.0

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Vorstellung der zukünftigen Inhalte im Kapitel 2 Datenschutz**

Copyright © · All rights reserved.

# Details Themen Datenschutz aus Kapitel 2

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Unabhängig von einem einzelnen oder gemeinsamen DSB stehen große Herausforderungen für Organisationen aller Art an**
  - Verantwortlichkeiten schaffen (Leitungsebene) – 2.1
  - DSB bestellen / benennen, sofern nicht vorhanden - 2.2
  - Dienstanweisung / Richtlinie Datenschutz - 2.3
  - Verzeichnis der Verarbeitungstätigkeiten - 2.4
  - Auftragsverarbeitung - 2.5
  - Informationspflichten nach Art. 13 und 14 DSGVO - Sidestep
  - Meldepflicht für Datenpannen - 2.6
  - Anpassen von Richtlinien, Dienstanweisungen und Dienstvereinbarungen - 2.7
  - Kontaktdaten des DSB veröffentlichen – 2.8
  - Datenschutz-Folgenabschätzung (DSFA) – 2.9
- **Achtung: keine abschließende Liste**

Copyright © · All rights reserved.

# 2.1 - Verantwortlichkeiten schaffen

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Organisationsleitung ist gefordert**
- **Datenschutz und Informationssicherheit sind CHEFSACHE**
- **Mehr Auflagen und Verantwortlichkeiten für Organisationsleitung**
  - Umsetzung kann teilweise delegiert werden
  - Haftung nicht!
- **Generell mehr Einsatz der Verantwortlichen in der Organisation gefordert**
  - Datenschutzbeauftragter auf zwei Funktionen reduziert
    - Beratung
    - Überwachung / Kontrolle
  - Umsetzung obliegt Organisationsleitung sowie delegierten Fach-/ Sachbereichen

Copyright © · All rights reserved.

# 2.2 – Benennung des Datenschutzbeauftragten

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Bestellpflicht für einen Datenschutzbeauftragten für alle öffentlichen Stellen**
- **Ab dem 25.05.2018 externe Bestellmöglichkeit für bayerische kommunale Einrichtungen auf Basis eines Dienstleistungsvertrages**
- **Datenschutzbeauftragter**
  - Berät
  - Überwacht
  - Kontrolliert
- **Weitere Aufgaben können delegiert werden, aber**
- **Vermeidung von Interessenskonflikten ist gesetzlich vorgeschrieben**
- **Beispiele:**
  - Führen des Verzeichnisses von Verarbeitungstätigkeiten kann delegiert werden. Nicht jedoch die Pflicht zur Lieferung der notwendigen Informationen aus den Fachbereichen
  - Risikofolgenabschätzung kann nicht delegiert werden. DSB hat Kontrollfunktion, ob diese korrekt durchgeführt wurde.
  - Durchführen von Mitarbeiterschulung und Sensibilisierungen kann delegiert werden. Kein Interessenskonflikt. Im Gegenteil: Know How aus erster Hand

Copyright © · All rights reserved.

# 2.2 – Benennung des Datenschutzbeauftragten

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Mehrere öffentliche Stellen können einen gemeinsamen Datenschutzbeauftragten bestellen**
  - Vorteile:
    - Zeitliche Auslastung
    - Im Thema
    - Schneller Aufbau von Erfahrung
    - Durch 100% Zeitanteil Vermeidung von Interessenskonflikten durch mehrere Aufgaben
  - Zu beachten:
    - Diener mehrerer Herren
    - Datenschutz kostet Zeit – Anzahl zu betreuender Stellen muss realistisch bleiben
- **Vertretungsregelung nicht vergessen!**
- **Unterschied kommunaler Datenschutz zu Unternehmensdatenschutz**
  - Für alle gilt die EU DSGVO!

Copyright © · All rights reserved.

# 2.3 Dienstanweisung Datenschutz

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Geschäftsanordnung / Dienstanweisung / Richtlinie**
  - Nennen Sie es, wie Sie wollen, Hauptsache es ist vorhanden und in Kraft
- **Ziele**
  - Klare Benennung der Zuständigkeiten und Verantwortlichkeiten
  - Vermeidung von „Nicht mein Tisch“
  - Klarstellung, mit Bestellung des DSB ist es für die Organisation nicht getan
- **Inhalte**
  - Darstellung Verantwortlichkeiten und Aufgaben
  - Alle Beschäftigte tragen gleichzeitig eine unmittelbare Verantwortung
  - Alle Dienststellen haben den DSB bei der Ausübung seiner Befugnisse und Erledigung seiner Aufgaben zu unterstützen
  - Kann um konkrete Handlungsanweisungen zum Datenschutz ergänzt werden (jedoch keine Wiederholung von Sachverhalten z.B. aus IuK Richtlinie)
- **Vorlage vom Bayerischen Staatsministerium des Innern, für Bau und Verkehr soll folgen**

Copyright © · All rights reserved.

# 2.4 – Verzeichnis der Verarbeitungstätigkeiten

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- Ersetzt das bisherige Verfahrensverzeichnis
- Wegfall der bisherigen Verfahrensfreigabe
- Dafür: Dem behördlichen DSB muss Gelegenheit zur schriftlichen Stellungnahme VOR Einsatz des Verfahrens gegeben werden -> rechtzeitige Einbindung notwendig
- Übersicht über automatisierte Verarbeitung personenbezogener Daten (Programme / Fachverfahren) sowie nicht-automatisierte Verarbeitung, deren Ergebnis im „Dateisystem“ gespeichert wird (Karteikarten, Register etc.)
- Elementarer Bestandteil der Rechenschaftspflicht (Art. 5 DSGVO) über die Rechtskonformität der Verarbeitung personenbezogener Daten („Wir sind eine Behörde“ reicht als Rechtsvorschrift nicht aus)
- Bisheriges Verfahrensverzeichnis kann mit überschaubarem Aufwand ergänzt werden, sofern aktuell und vollständig

Copyright © · All rights reserved.

# 2.4 – Verzeichnis der Verarbeitungstätigkeiten

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Dokumentation des eigenen Schutzniveaus (TOM) mit https://www.bdsg-externer-datenschutzbeauftragter.de/auftragsverarbeitung/ueberpruefung-externe-dienstleister-im-rahmen-der-auftragsverarbeitung-nach-art-28-dsgvo-tom/**
- **Keine Veröffentlichungspflicht, Recht auf Einsichtnahme für Landesdatenschutzbehörde, Informationszugangsrecht / Auskunftsbegehren im Einzelfall zu prüfen**
- **Verzeichnis Dreh- und Angelpunkt der Tätigkeit des DSB**
  - Prüfen der rechtskonformen Verarbeitung personenbezogener Daten in der Organisation
  - Auskunftspflicht (wo suchen, wenn Betroffener sein Auskunftsrecht wahrnimmt)
  - Informationspflichten (Angaben für Pflichtangaben aus Art. 13 und 14 DSGVO stehen im Verzeichnis)
  - Anfrage der Landesdatenschutzbehörde
  - Keine reine “Abheft-Funktion“ mehr
- **Nicht vom Gesetz und in den meisten Vorlagen vorgesehen, aber mehr als sinnvoll in der Praxis: Verzeichnis um Angaben zu externen Dienstleistern ergänzen -> Durchführen und Überwachen der Auftragsverarbeitung**

Copyright © · All rights reserved.

# 2.5 - Auftragsverarbeitung

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Kennen wir als Auftragsdatenverarbeitung aus dem bisherigen Datenschutz-Recht**
- **Dienstleister erhält personenbezogene Daten von Organisation oder hat im Rahmen seiner Tätigkeit (theoretische) Zugriffsmöglichkeit darauf -> Auftragsverarbeitung**
- **Einführung eAkte, Scandienst, Entsorgung, Vor-Ort-Service, Fernwartung / IT Support, Auslagerung ins Rechenzentrum, Cloud-Services und viele, viele mehr …**
- **Auftraggeber hat folgende Schritte durchzuführen (Reihenfolge beachten!):**
  - Prüfen des Dienstleisters auf ausreichendes Schutzniveau
  - Dokumentation der Prüfergebnisse
  - Abschluss einer schriftlichen Vereinbarung zur Auftragsverarbeitung neben dem eigentlichen Vertrag
  - Beginn der Zusammenarbeit
- **Keine Ausnahmeregelung für bestimmte Dienstleister**

Copyright © · All rights reserved.

# 2.5 - Auftragsverarbeitung

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Vorgehensweise ist in der EU DSGVO festgelegt**
- **Vorlagen dazu existieren**
  - Prüfen des Schutzniveaus z.B. mit https://www.bdsg-externer-datenschutzbeauftragter.de/auftragsverarbeitung/ueberpruefung-externe-dienstleister-im-rahmen-der-auftragsverarbeitung-nach-art-28-dsgvo-tom/
  - Vereinbarung zur Auftragsverarbeitung mit https://www.datenschutz-guru.de/download/15413/
  - Sonderfall IT-Wartung mit https://www.datenschutz-guru.de/download/7702/
- **Kein Abwarten auf andere Vorlagen notwendig, da DSGVO das Thema inhaltlich abschließend regelt**

Copyright © · All rights reserved.

# Sidestep – Informationspflichten Art. 13, 14 DSGVO

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Problematisches Thema, da neu und keine praktischen Erfahrungen für alle Beteiligten**
- **Zu unterscheiden**
  - Die Informationspflicht bei der Erhebung bei der betroffenen Person (Art. 13 DSGVO)
  - Die Informationspflicht bei der Erhebung nicht bei der betroffenen Person (Art. 14 DSGVO)
  - Die Informationspflicht bei einer Zweckänderung vorhandener personenbezogener Daten (Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO)
- **Informationspflicht besteht nicht, soweit die betroffene Person bereits über die Informationen verfügt**
  - Verwaltungsverfahren / feste Prozesse reicht Information 1 x zu Beginn
- **Beispiele**
  - Erhebung mittels Papierformular / Antrag (z.B. Rückseite oder mit separatem Handzettel)
  - Erhebung auf Webseite / Online-Formular (z.B. im Rahmen der Datenschutz-Erklärung)
  - Erhebung bei mündlicher Befragung oder am Telefon (da fehlte den Machern der DSGVO der Praxisbezug!)
    - Entweder Rechte am Telefon vorlesen
    - Bandansage vor Annahme des Telefonats (Vorschlag einer Landesdatenschutzbehörde)
    - Kurzer Hinweis zu Beginn des Telefonats mit Verweis auf alle Detailinformationen z.B. auf Webseite (Medienbruch, wird aktuell noch kritisch diskutiert)

Copyright © · All rights reserved.

# Sidestep – Informationspflichten Art. 13, 14 DSGVO

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Vorlagen zu den notwendigen Angaben z.B.**
  - Leitfaden Datenschutz Reform für kommunale Einrichtungen
    https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php
  - Gesellschaft Datenschutz und Datensicherheit (recht pragmatischer Ansatz)
    https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf
- **Ab 25.05.2018 jederzeit von außen überprüfbar durch**
  - Angaben auf Webseite
  - Testanruf
- **Wir müssen das Thema ernst nehmen, auch wenn noch keiner so richtig weiß, wie es funktioniert!**

Copyright © · All rights reserved.

# 2.6 – Meldepflicht Datenpannen

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Datenpanne mit personenbezogenen Daten Meldung an https://www.datenschutz-bayern.de/service/data_breach.html**
- **Frist 72h nach Bekanntwerden**
- **Ausnahme: Wenn Datenpanne nicht zu einem Risiko für die Freiheiten und Rechte der betroffenen Person(en) führt**
- **Umfassende Liste von zu meldenden Datenpannen (nicht abschließend)**
  - Gerät oder Unterlagen verloren
  - Unverschlüsselter Email-Versand (besondere Kategorien personenbezogener Daten oder Steuer- oder Sozialdaten)
  - Verlust oder versehentliche Öffnung Postsendung
  - Hackerangriff, Schadcode, Phishing
  - Nicht rechtskonforme Entsorgung analoger / digitaler Datenträger (Papier, Sticks, Festplatten …)
  - Unbeabsichtigte Veröffentlichung
  - Personenbezogene Daten an falschen Empfänger versandt

Copyright © · All rights reserved.

# 2.6 – Meldepflicht Datenpannen

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Ursachen für Datenpannen für die Informationssicherheit von großem Interesse**
  - Analyse der Ursache
  - Planung und Einführung von Maßnahmen zur Vermeidung identischer oder ähnlicher Datenpannen
- **Wichtig: Es geht dabei nicht darum, wer schuld ist, sondern was zur Datenpanne geführt hat (Umdenken erforderlich)**
- **Zusätzlich Meldepflicht nach Art. 11 Abs. 2 BayEGovG an LSI und oberste Dienstbehörde bei Anschluss an Behördennetz (unverzüglich)**

Copyright © · All rights reserved.

# 2.7 – Anpassen von Richtlinien und DA

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

## ► Notwendig, sofern

- Rechtsbezug zu altem und somit ungültigem Gesetz besteht.
- diese nicht mehr den aktuellen Sicherheitsanforderungen oder dem Stand der Technik entsprechen.

Copyright © · All rights reserved.

# 2.8 – Kontaktdaten des DSB veröffentlichen

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Die Kontaktdaten des DSB müssen auf der Webseite der Organisation veröffentlicht werden**
  - Keine Namensnennung
  - Anschrift / Telefon / Fax / Email z.B. datenschutz@
  - Leichte Erreichbarkeit
  - Nicht verstecken
- **Weiterhin Pflicht zur Meldung des DSB bei der Landesdatenschutzbehörde**
  - Online-Formular https://www.datenschutz-bayern.de/service/bdsb.html
- **Und falls jemand noch keine hat: Datenschutzerklärung gleichberechtigt zum Impressum**
- **Alles von außen leicht nachprüfbar, daher bis 25.05.2018 erledigen**

Copyright © · All rights reserved.

# 2.9 – Datenschutz-Folgenabschätzung (DSFA)

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Generell notwendig:**
  - Risikobewertung bei neuen Verfahren oder weitreichenden Änderungen an bestehenden Verfahren
  - Stellungnahme des DSB
  - Schutzklassen / Risikoklassen / Schadensszenarien zu definieren
- **Bei Erreichen der höchsten Risikoklasse**
  - Durchführen einer Datenschutz-Folgenabschätzung
  - Beispielsweise bei
    - Umfangreicher Verarbeitung besondere Kategorien personenbezogener Daten
    - Umfangreiche Videoüberwachung bei öffentlich zugänglichen Räumen
    - aber wohl auch Meldewesen (Schutzdaten / Sperrvermerke) und vergleichbare Verfahren
- **Explizite und detaillierte Prüfung, ob vorhandene technische und organisatorische Maßnahmen für das risikoreiche Einzelverfahren ausreichend sind**
- **Konkrete Vorgehensweise noch unklar. Grundlage könnte ein ISMS wie BSI IT-Grundschutz oder ISIS12 sein**
- **Übergangsfrist bis voraussichtlich 2021**
- **Aufgrund der Anforderungen an TOM und Vorgehensweise enge Verzahnung mit Informationssicherheit**

Copyright © · All rights reserved.

# Es gibt viel zu tun

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Alleine die Anforderungen aus der DSGVO im Bereich Datenschutz machen eine Überarbeitung der Arbeitshilfe notwendig**
- **Abwarten vergrößert das Problem**
  - Weite Teile der Anforderungen sind bekannt und können bereits umgesetzt werden
  - Es wird nicht für jede Aufgabe eine Mustervorlage benötigt, um anzufangen
  - „Bayerische Vorlagen“ sind ebenfalls nicht zwingend notwendig, da die meisten Punkte abschließend durch die DSGVO geregelt sind und sehr brauchbare und pragmatische Lösungen existieren
- **Problem:**
  - Eigenleistung notwendig
  - Zitat Landesdatenschutzbeauftragter BW: „Wer sich vor 2 Jahren keine externe Unterstützung gesichert hat, schaut in die Röhre. Der Markt an externen Beratern ist aktuell leergefegt“.
  - Gute Nachricht: Es stocken alle Personal auf so gut es geht
- **Doch nun zur Arbeitshilfe generell in der Praxis**

Copyright © · All rights reserved.

# Die Arbeitshilfe im praktischen Einsatz

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- *„Geeignetes Mittel für kleinere Kommunen, um ein Informationssicherheitskonzept einzuführen.“*
- *„Klare und strukturierte Gliederung“*
- *„Verständlich formuliert, auch für Nicht-IT-Profis“*
- *„Übersichtliche Darstellung der Schwachstellen und Bewertung“*
- *„Gelungener Einstieg über Leitlinie Informationssicherheit in Verbindung mit IuK Richtlinie“*
- *„Bearbeitung / Umsetzung im Team hilft ungemein“*
- *„Bei Bedarf externe Dienstleister z.B. bei IT-Themen hinzuziehen“*
- *„Vertretbarer Aufwand“*
- *„Klare Weiterempfehlung“*

Copyright © · All rights reserved.

# Umsetzungsmöglichkeiten

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Gedacht als Hilfe zur Selbsthilfe**
- **Benötigt wird Ausdruck der Arbeitshilfe, Stift und etwas Zeit**
- **Arbeitshilfe selbst nur als Word-Formular ausgelegt**
  - Erster Durchlauf zur Dokumentation von Schwachstellen und Maßnahmenplanung unkritisch
  - Eher ungeeignet für langfristigen Betrieb:
    - Dokumentation wird immer umfangreicher (Schwachstelle Word)
    - Keine automatisierten Wiedervorlagen
    - Keine Reporting-Möglichkeit
- **Erste Software-Unterstützung vorhanden**
  - Webbasierte Anwendung
  - Immer die aktuelle Arbeitshilfe zur Bearbeitung
  - Aufgaben- und Terminplanung
  - Zuweisung von Verantwortlichkeiten (inkl. Aufgabenlisten)
  - Ansprechpartner: Datenschutz Schmidt GmbH & Co KG Lauf

Copyright © · All rights reserved.

# Zeitaufwand

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Konsequente Bearbeitung intern**
  - Arbeitshilfe am Stück lesen, Notizen machen: 1 Tag
  - Schwachstellenidentifikation, Interviews, Nachfragen: 3-4 Tage
  - Mitarbeitersensibilisierung 0,5-1 Tage
  - Planen von Schutzmaßnahmen: 1-2 Tage
  - Umsetzung: kommt drauf an ☺
- **Bei Bedarf externe Unterstützung heranziehen**
  - Verständnisfragen -> Informationssicherheitsberater
  - Beantwortung IT Fragen -> externer IT-Dienstleister (sofern genutzt)
  - Planung und Konzeption von Maßnahmen -> Informationssicherheitsberater
  - Mitarbeiterschulung -> Externer Trainer
  - Umsetzung einzelner Maßnahmen

Copyright © · All rights reserved.

# Workshop-Konzept statt Einzelkämpfer

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

Anleitung, Tipps / Tricks

Umsetzung

Status

Rückfragen

Copyright © · All rights reserved.

# Workshops Arbeitshilfe – Möglicher Fahrplan

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

- **Workshop 1 – Auftaktveranstaltung**
  - Grundlagen
  - Vorstellung Software-Unterstützung
  - Vorstellung und Besprechung der Kapitel und Hausaufgaben bis Workshop 2
    - Kapitel 1 – Informationssicherheit
    - Kapitel 2 – Datenschutz
- **Workshop 2**
  - Besprechung Ergebnisse / Status Quo Hausaufgaben
  - Einweisung ausgewählte Softwarelösung
  - Vorstellung und Besprechung der Kapitel und Hausaufgaben bis Workshop 3
    - Kapitel 3 – Gebäudesicherheit (Begehung z.B. durch Externe, Stichwort Betriebsblindheit)
    - Kapitel 4 – Zugang zu IT-Systemen
- **Workshop 3**
  - Besprechung Ergebnisse / Status Quo Hausaufgaben
  - Vorstellung und Besprechung der Kapitel und Hausaufgaben bis Workshop 4
    - Kapitel 5 - Berechtigungskonzepte und Protokollierung
    - Kapitel 6 - Notfallmanagement
    - Kapitel 7 - Richtlinien und Dienstanweisungen

Copyright © · All rights reserved.

# Workshops Arbeitshilfe – Möglicher Fahrplan

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Workshop 4**
  - Besprechung Ergebnisse / Status Quo Hausaufgaben
  - Vorstellung und Besprechung der Kapitel und Hausaufgaben bis Workshop 5
    - Kapitel 8 - Schulungen und Sensibilisierung – Mitarbeiter als elementarer Bestandteil der Informationssicherheit
  - Durchführen der Schulungen (intern / extern)
- **Workshop 5**
  - Besprechung Ergebnisse / Status Quo Hausaufgaben
  - Vorstellung und Besprechung der Kapitel und Hausaufgaben bis Workshop 6
    - Kapitel 9 – Externe Dienstleister
- **Workshop 6**
  - Besprechung Ergebnisse / Status Quo Hausaufgaben
  - Vollständigkeitsprüfung / Erfolgskontrolle
  - Betreuungskonzept / Sicherstellung des Betriebs des Informationssicherheitskonzepts (intern / extern)
- **Dazwischen Mitarbeiterschulungen (zentral für alle)**

Copyright © · All rights reserved.

# Workshop-Modelle

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

- **Landkreis Wunsiedel**
  - Alle Landkreis-Kommunen (Städte und Gemeinden)
  - Unter Anleitung und mit Unterstützung vom Landratsamt
  - Bereits gestartet, Workshop 3 in 05/18
- **Landkreis Cham**
  - Alle Landkreis-Kommunen (Städte und Gemeinden)
  - Unter Anleitung und mit Unterstützung vom Landratsamt
  - Start in 06/18
- **Kommunale Allianzen**
  - Diverse im Vorlauf

Copyright © · All rights reserved.

# Man glaubt es kaum

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

Datenschutz und Informationssicherheit sind Aufgabe der ganzen Organisation / aller Mitarbeiter.

DSB / ISB wirken auf Sicherstellung hin (Beratung) und üben Kontrollfunktion aus.

DSB / ISB setzen selbst nicht / kaum um -> Vermeidung von Interessenskonflikten (gesetzliche Vorschrift! beim DSB).

Datenschutz und Informationssicherheit kosten Zeit (da ist nichts mit „Nebenher“).

Copyright © · All rights reserved.

# VIEL ERFOLG BEI DER UMSETZUNG

Copyright © · All rights reserved.