

**OPEN  
RHEIN  
RUHR**



# **DSGVO IT SICHERHEITSDOKUMENTE MIT VERINICE VERWALTEN**

[hagen.bauer@rusticus-consulting.de](mailto:hagen.bauer@rusticus-consulting.de)

# ÜBER MICH

- Hagen Bauer
- IT Berater (Software / Infrastruktur)
- Datenschutzfreak
- Freifunker
- Serveradministrator
- Webseiten Programmierer
- Web Shop Administrator



**DISCLAIMER:**

**DIESE INFORMATIONEN SOLLEN NUR HELFEN DAS RICHTIGE  
ZU TUN.**

**SIE ERSETZEN KEINE RECHTSBERATUNG UND ERHEBEN KEINEN ANSPRUCH AUF  
VOLLSTÄNDIGKEIT UND/ODER RICHTIGKEIT.**

# DIE DATENSCHUTZGRUNDVERORDNUNG

- 2016 durch EU festgelegt
- ersetzt die Datenschutzrichtlinie aus dem Jahr 1995
- ist in der gesamten EU als Gesetz anerkannt
- Mitgliedstaaten mussten bis Mai 2018 Umsetzung sicherstellen



# NEUE ANFORDERUNGEN

- neue Datenschutzerklärung auf Webseiten notwendig
- Vertrag zur Auftragsverarbeitung für externe Dienstleister
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzbeauftragter bei besonders geschützten Daten
- Weitere Rechte des Verbrauchers (Auskunft, Löschung, Übertragung...)
- Meldepflicht von Vorfällen

# UND DAS IST AUCH RICHTIG SO

**welt**

 Abonnement

 4 Ticker

 Suche

 Login

HOMEWELTPLUSLIVE-TV  
MEDIATHEK  
POLITIK  
WIRTSCHAFT  
SPORT  
PANORAMA  
WISSEN  
KULTUR  
M  
MEHR >PRODUKTE

HOME » REGIONALES » NORDRHEIN-WESTFALEN » Häftling findet in JVA Euskirchen Stick mit sensiblen Daten

## NORDRHEIN-WESTFALEN

POLITIK IN NRW   WETTER IN NRW   STELLENANGEBOTE

NORDRHEIN-WESTFALEN   JVA EUSKIRCHEN

### Häftling findet Stick mit sensiblen JVA-Mitarbeiter-Daten

Ein Gefängnis-Mitarbeiter verliert einen USB-Stick – ausgerechnet mit sensiblen Daten vieler JVA-Bediensteter. Ein Häftling findet ihn – und will ihn wieder verloren haben. Wo sich der Stick derzeit befindet, sei unklar.

3

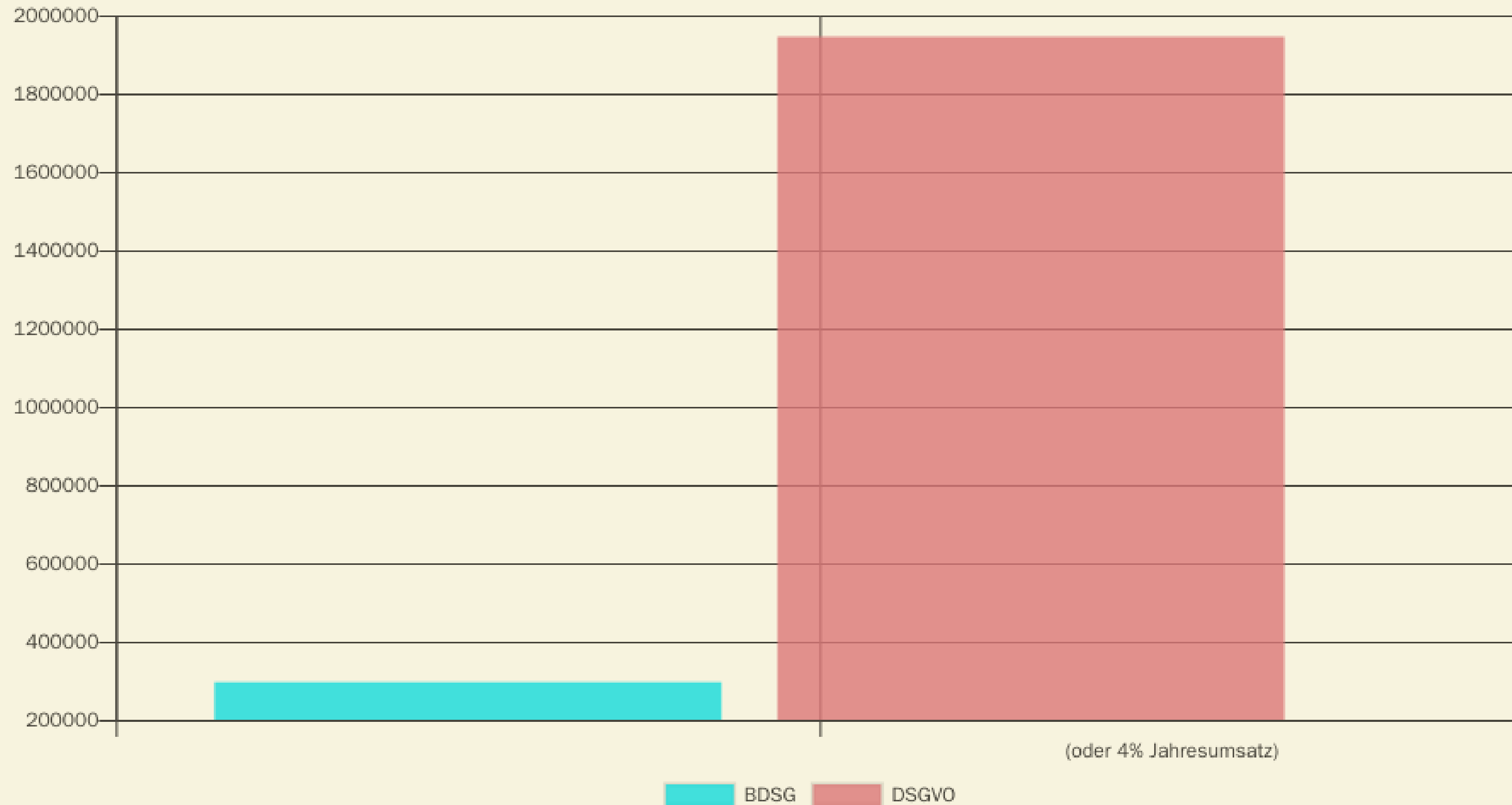




E

in verlorener USB-Stick mit sensiblen persönlichen Daten von rund 80 Vollzugsbeamten des Gefängnisses Euskirchen ist ausgerechnet in die Hand eines Häftlings gelangt. „Der Stick ist gefunden worden, von einem

# DATENSCHUTZ MIT ZÄHNEN



# UND NICHT NUR IN DER THEORIE



IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal

heise online › News › 10/2018 › DSGVO-Verstoß: Krankenhaus in Portugal soll 400.000 Euro zahlen

23.10.2018 11:06 Uhr

## DSGVO-Verstoß: Krankenhaus in Portugal soll 400.000 Euro zahlen

In einem Krankenhaus in Portugal hatten nicht nur Ärzte Zugriff auf Patientendaten. Dafür wurde nun eine empfindliche Geldstrafe verhängt.

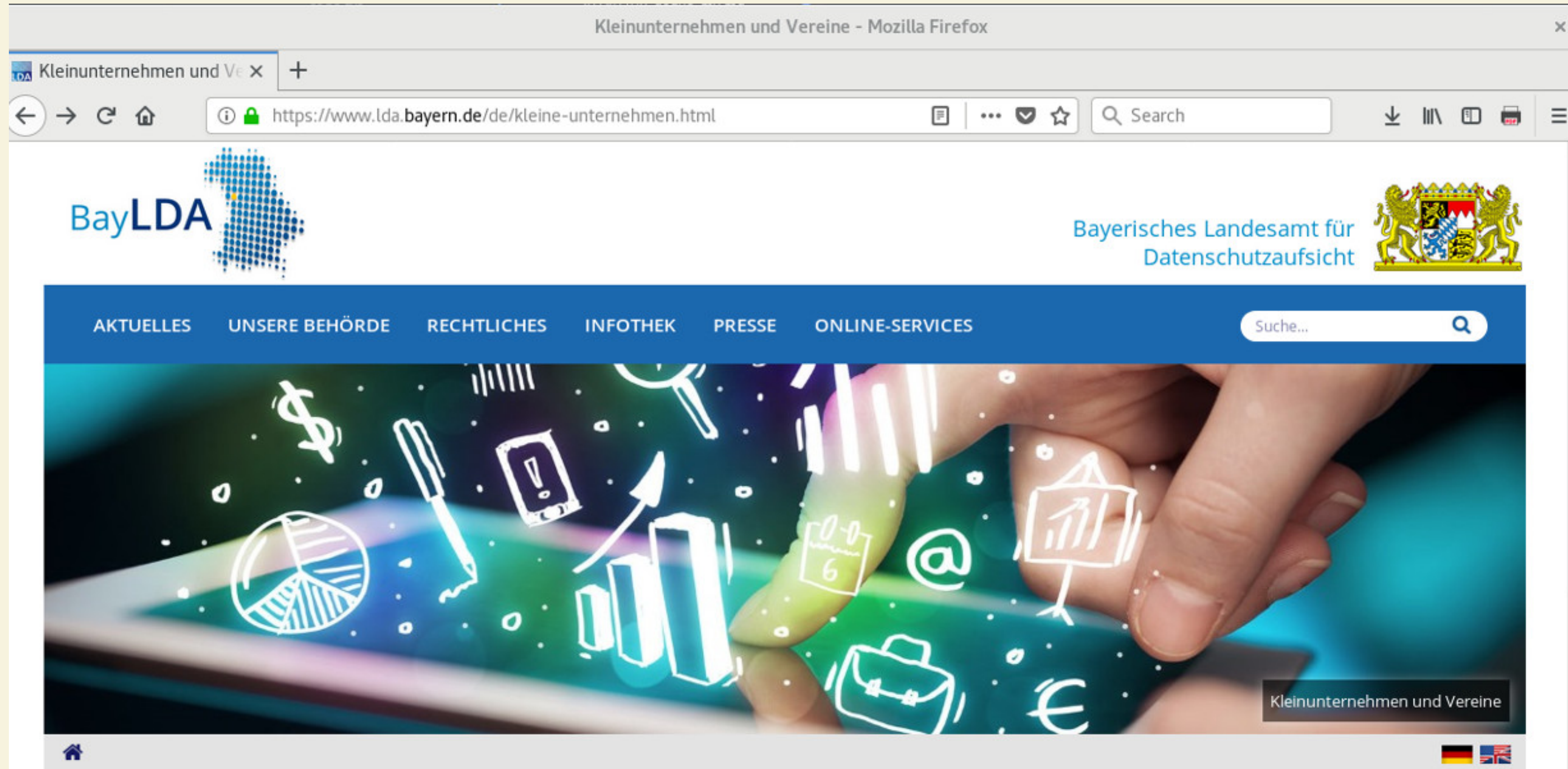
- z.B. 985 aktive Benutzer mit einem Profil "Arzt" bei 296 Ärzten



# VEREINFACHTE TODO LISTE

| Tätigkeit                                            | Prio | Aufw. |
|------------------------------------------------------|------|-------|
| Datenschutzerklärung/Cookie Banner<br>/ Social Media | 1    | N     |
| Datenschutzbeauftragter?                             | 1    | N     |
| Verzeichnis von<br>Verarbeitungstätigkeiten          | 2    | H     |
| Prozess für Auskunft/Löschen                         | 2    | M     |
| Basis IT Sicherheitskonzept                          | 2    | M     |
| Datenschutzfolgeabschätzung                          | 3    | H     |

# GUTE HILFESTELLUNGEN AUS BAYERN



## Handreichungen für kleine Unternehmen und Vereine

In der folgenden Übersicht werden für kleine Unternehmen und Vereine die wesentlichen Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesen Mustern wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den Anforderungen befinden sich auf der Rückseite des jeweiligen Papiers.

# PFLICHT: IT SICHERHEITSKONZEPTION

- z.Z. Keine "handhabbaren" Standards
- Stand der Technik???
- BSI IT Grundschutz bietet eine systematische Herangehensweise
- Pragmatische Auslegung möglich



# DIE IDEE HINTER DEM BSI GRUNDSCHUTZ

- Wiederverwendbarkeit, Anpassbarkeit, Erweiterbarkeit
- Benennung der typischen
  - Gefährdungen, Schwachstellen und Risiken
  - Geschäftsprozesse und Anwendungen
  - IT-Komponenten
- Empfehlungen und Maßnahmen werden bereitgestellt
- Quelle



# VORGEHENSWEISE

1. IT-Sicherheitsprozess starten
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung nach IT-Grundschutz
5. Basis-Sicherheitsscheck
6. Realisierung von Sicherheitsmaßnahmen
7. Kontinuierliche Verbesserung

# GRUNDSCHUTZ MIT VERINICE

The screenshot displays the Verinice software interface. The top bar shows 'Aktivitäten', 'V. verinice', and the time 'Fr 13:31'. The main window is titled 'verinice' and contains a menu bar with 'Datei', 'Bearbeiten', 'Ansicht', and 'Hilfe'. Below the menu is a toolbar with various icons. The interface is divided into three main panes:

- Left Pane (IT-Grundschutz-Kompodium):** A tree view showing the hierarchy of IT security measures. The selected item is 'SYS.1.2.2.A3 Sichere Administration von Windows Server 2012'.
- Middle Pane (Modernisierter IT-Grundschutz):** A tree view showing the project structure. The selected item is 'Abteilungsserver'.
- Right Pane (Abteilungsserver):** A details pane for the selected 'Abteilungsserver' object. It contains fields for 'Kürzel' (S1), 'Titel' (Abteilungsserver), 'Tags', and 'Beschreibung'. Below these fields is a section for 'Verknüpfungen' (Links).

The 'Objektbrowser' (Object Browser) pane at the bottom right shows the selected object's details, including the title 'SYS.1.2.2.A3 Sichere Administration von Windows Server 2012' and a description: 'Lokale Administrationskonten MÜSSEN einzigartige, sichere Passwörter besitzen. Alle Administratoren, die für das Serversystem zuständig sind, MÜSSEN in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 bzw. R2 geschult sein. Sie DÜRFEN administrative Rechte NICHT einsetzen, wo diese nicht zwingend erforderlich sind. Browser auf dem Server DÜRFEN NICHT zum Surfen im Web verwendet werden.'

# VERINICE

- Open Source Information Security Management System (ISMS)
- GNU General Public License
- Windows, Linux and OS X
- Demo und Kaufversion auf Hersteller Webseite
- Quellcode auf <https://github.com/SerNet/verinice>

# DEMO



**ERGEBNISS: EIN BESSERER SCHUTZ DER DATEN MEINER  
ORGANISATION UND MEINER KUNDEN**







**OPEN  
RHEIN  
RUHR**



# **DSGVO IT SICHERHEITSDOKUMENTE MIT VERINICE VERWALTEN**

[hagen.bauer@rusticus-consulting.de](mailto:hagen.bauer@rusticus-consulting.de)