



# 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
- Jekyll Webseiten
- 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

The screenshot shows the top navigation bar of the 'welt' website. The logo 'welt' is on the left. On the right, there are links for 'Abonnement', 'Ticker' (with a notification icon), 'Suche', and 'Login'. Below the navigation bar is a horizontal menu with categories: HOME, WELTPLUS, LIVE-TV, MEDIATHEK, POLITIK, WIRTSCHAFT, SPORT, PANORAMA, WISSEN, KULTUR, M, MEHR >, and PRODUKTE. The breadcrumb trail reads: HOME » REGIONALES » NORDRHEIN-WESTFALEN » Häftling findet in JVA Euskirchen Stick mit sensiblen Daten. The main heading is 'NORDRHEIN-WESTFALEN' with sub-links for 'POLITIK IN NRW', 'WETTER IN NRW', and 'STELLENANGEBOTE'. The article title is 'Häftling findet Stick mit sensiblen JVA-Mitarbeiter-Daten'. The sub-headers are 'NORDRHEIN-WESTFALEN' and 'JVA EUSKIRCHEN'. The text of the article begins with: '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.' Below the text, there is a large letter 'E' followed by the text: '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'. On the left side of the article, there is a small number '3' and a Facebook icon.

welt

Abonnement Ticker Suche Login

HOME WELTPLUS LIVE-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

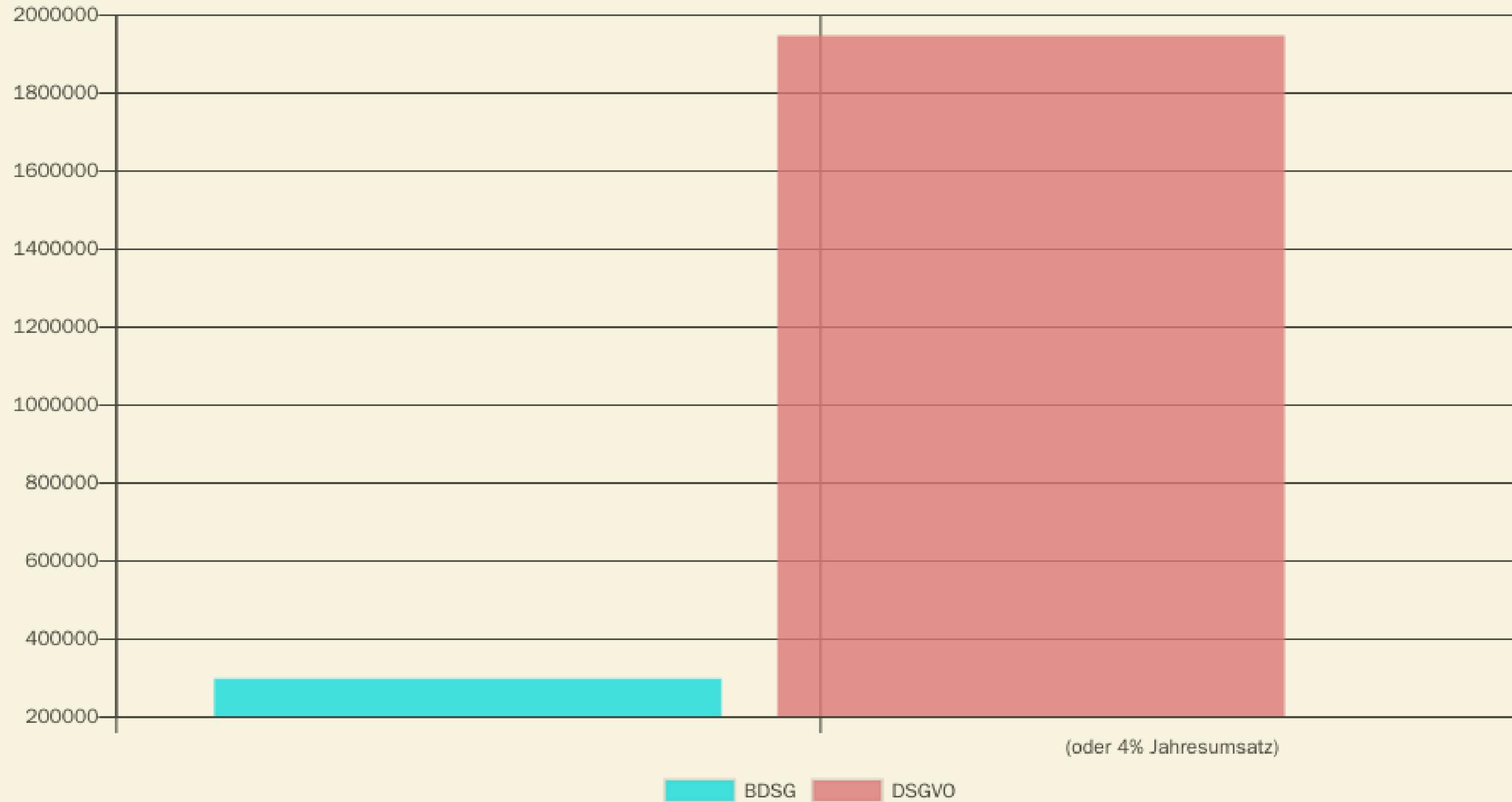
### Häftling findet Stick mit sensiblen JVA-Mitarbeiter-Daten

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 / Social Media	1	N
Datenschutzbeauftragter?	1	N
Verzeichnis von Verarbeitungstätigkeiten	2	H
Prozess für Auskunft/Löschen	2	M
Basis IT Sicherheitskonzept	2	M
Datenschutzfolgeabschätzung	3	H

# GUTE HILFESTELLUNGEN AUS BAYERN

The screenshot shows a Mozilla Firefox browser window with the address bar displaying <https://www.lda.bayern.de/de/kleine-unternehmen.html>. The page header features the BayLDA logo on the left and the Bayerisches Landesamt für Datenschutzaufsicht logo on the right. A navigation menu includes links for AKTUELLES, UNSERE BEHÖRDE, RECHTLICHES, INFOTHEK, PRESSE, and ONLINE-SERVICES, along with a search bar labeled 'Suche...'. The main content area is a large banner image showing a hand interacting with a tablet displaying various business-related icons like a pie chart, bar graph, and currency symbols. A small text box in the bottom right of the banner reads 'Kleinunternehmen und Vereine'. At the bottom of the banner, there are flags for Germany and the UK.

## 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 / ITGrundschutzkompendium

# VORGEHENSWEISE

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

# GRUNDSCHUTZ MIT VERINICE

The screenshot displays the Verinice software interface. The top bar shows the application name 'verinice' and the system clock 'Fr 13:31'. The main window is divided into several panes:

- IT-Grundschutz-Kompodium 3.0:** A tree view showing the hierarchy of IT security components. The 'System-Bausteine' section is expanded, showing 'SYS.1.2.2 Windows Server 2012' selected.
- Modernisierter IT-Grundschutz:** A tree view showing the modernized IT security components. The 'Abteilungsserver' component is selected.
- Abteilungsserver:** A detailed view of the selected component, showing fields for 'Kürzel' (S1), 'Titel' (Abteilungsserver), 'Tags', and 'Beschreibung'.
- Objektbrowser:** A pane showing the selected component'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
- Einzelplatz und Serverversion verfügbar
- Quellcode auf <https://github.com/SerNet/verinice>

# DEMO

■ ■

# OFFENE PUNKTE

- Holistische Abdeckung DSGVO Anforderungen erfordert Zusatzmodul oder Eigenentwicklung
- Installation und Einrichtung OpenSource Version ist "hackelig"

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





# DSGVO IT SICHERHEITSDOKUMENTE MIT VERINICE VERWALTEN

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