

DIE DSGVO ALS CHANCE NUTZEN

EIN FAHRPLAN FÜR EIN MEHR AN INFORMATIONSSICHERHEIT IN KLEINEN SCHRITTEN

hagen.bauer@rusticus-consulting.de @hagen_bauer

ÜBER MICH

- Hagen Bauer
- Freiberuflicher IT Berater
- Datenschutzfreak
- Freifunker
- Serveradministrator
- Web Shop Betreiber



DISCLAIMER:

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

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

AGENDA

- Informationssicherheit ist finanziell bewertbar
- Ein Fahrplan wird bereitgestellt
- Informationssicherheit bedarf einer ständigen Überwachung
- Aufrechterhaltung der Informationssicherheit ist ein neues geschäftsrelevantes Aufgabenfeld

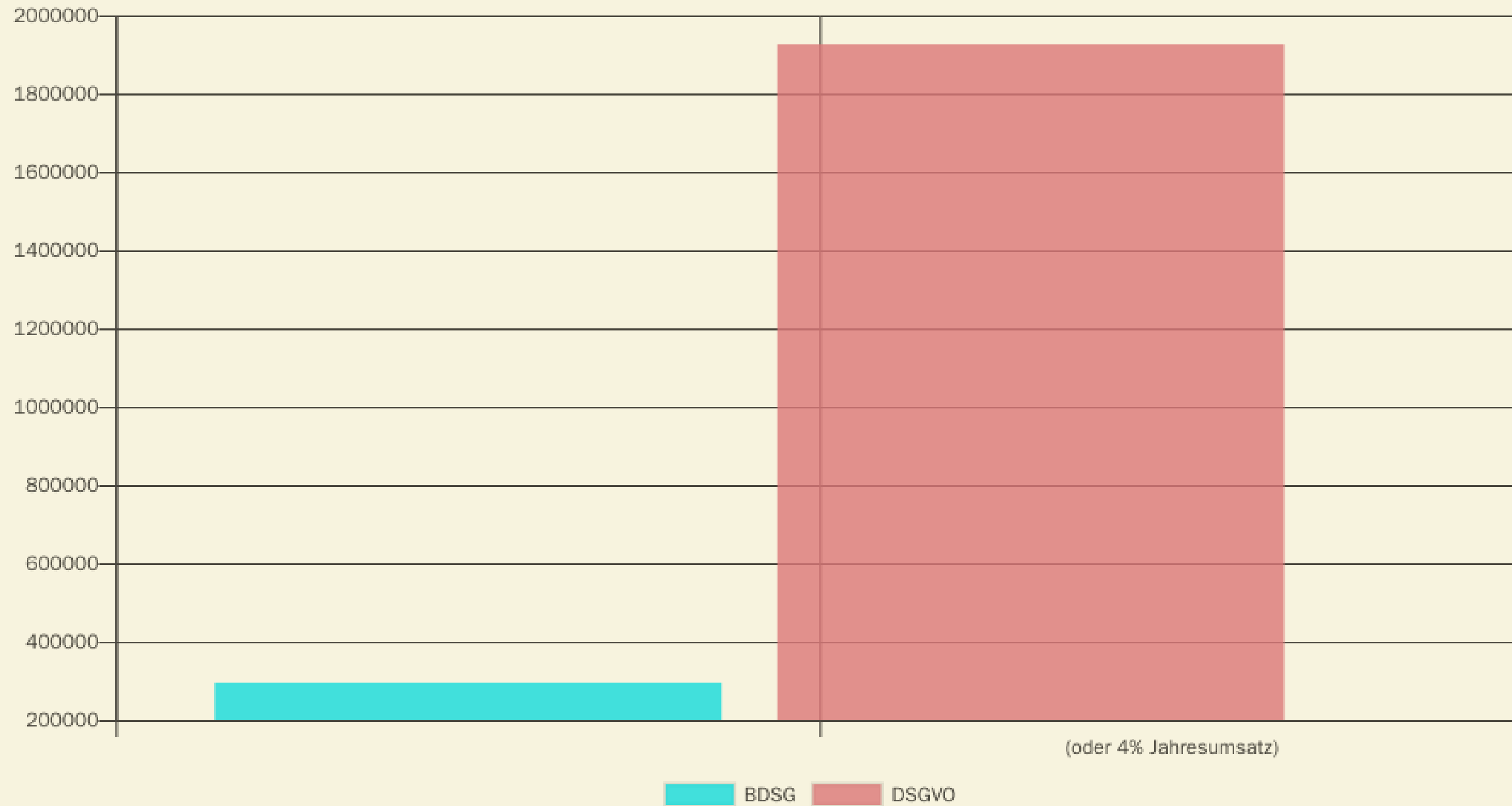
DIE DATENSCHUTZGRUNDVERORDNUNG

- 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

AKTUELLER STAND IST ERSCHÜTTERND
30% TEILWEISE ODER
GAR NICHT

- TÜV Süd Mai 2019

DATENSCHUTZ MIT ZÄHNEN



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

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

UND NICHT NUR IN DER THEORIE



1/7

936-150719

Procedimiento Nº: PS/00300/2019

RESOLUCIÓN R/00499/2019 DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

En el procedimiento sancionador PS/00300/2019, instruido por la Agencia Española de Protección de Datos a **VUELING AIRLINES, S.L.**, vista la denuncia presentada por **A.A.A.**, y en base a los siguientes,

ANTECEDENTES

- Bußgeld über 30.000 Euro wegen Cookie-Banner

UND NICHT NUR IN DER THEORIE

BBC  Sign in News Sport Reel Worklife Travel Future

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

UK watchdog plans to fine Marriott £99m

 9 July 2019      Share

The UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m.

The penalty relates to a data breach that resulted in about 339 million guests having had their personal details exposed.

The incident is thought to date back to 2014 but was only discovered in 2018.

It comes a day after the Information Commissioner's Office (ICO) said it planned to fine British Airways £183m over a separate breach.

TYPISCHE VERDRÄNGUNGSSTRATEGIEN

**"DAS IST MIR EGAL.
ICH VERKAUFE EH IN 5 JAHREN"**

GARTNER: CYBERSECURITY IS CRITICAL TO THE M&A DUE DILIGENCE PROCESS

UND NICHT NUR IN DER THEORIE

BBC  Sign in News Sport Reel Worklife Travel Future

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

UK watchdog plans to fine Marriott £99m

 9 July 2019      Share

The UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m.

The penalty relates to a data breach that resulted in about 339 million guests having had their personal details exposed.

The incident is thought to date back to 2014 but was only discovered in 2018.

It comes a day after the Information Commissioner's Office (ICO) said it planned to fine British Airways £183m over a separate breach.

ABER ICH WERDE SCHON NICHT GEHACKT

AKTUELLE HITLISTE

1. Postfehlversand
2. Hackingangriffe/Malware/Trojaner
3. E-Mail Fehlversand
4. Diebstahl eines Datenträgers
5. Versendung einer E-Mail mit offenem Adressverteiler
6. Verlust eines Datenträgers
7. Fax-Fehlversand
8. Quelle **LfDI July 2019**

**ICH BIN KLEIN, WIRD SCHON NICHT SO
TEUER WERDEN.**

KOSTEN EINES VORFALLS?

- "Cost-of-a-Data-Breach"-Studie IBM
- Unternehmen mit weniger als 500 Mitarbeitern

2,2 MIO. EURO PRO VORFALL

FEHLENDE INFORMATIONSSICHERHEIT BEDEUTET

- steigendes Risiko für empfindliche Strafen
- sinkende Unternehmenswerte
- steigende Versicherungskosten
- Risiken beim Kauf/Verkauf von Unternehmen oder Sparten

LÖSUNGSANSATZ: IT SICHERHEITSKONZEPTION

- 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 / IT-Grundschutzkompendium

VORGEHENSWEISE

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

GRUNDSCHUTZ MIT VERINICE

Aktivitäten V. verinice Fr 13:31 de

verinice

Datei Bearbeiten Ansicht Hilfe

IT-Grundschutz-Kompodium Modernisierter IT-Grundschutz Abteilungsserver

IT-Grundschutz-Kompodium 3.0

- Bausteine
 - Prozess-Bausteine
 - CON
 - DER
 - ISMS
 - OPS
 - ORP
 - System-Bausteine
 - APP
 - IND
 - INF
 - NET
 - SYS
 - SYS.1.1 Allgemeiner Server
 - SYS.1.2.2 Windows Server 2012
 - SYS.1.2.2.A1 Planung von Window
 - SYS.1.2.2.A2 Sichere Installation v
 - SYS.1.2.2.A3 Sichere Administrati
 - SYS.1.2.2.A4 Sichere Konfiguratio

Informationsverbund

- Geschäftsprozesse
 - Einkauf
- Anwendungen
 - msoffice
- IT-Systeme
 - Client-Einkauf
 - Abteilungsserver
- ICS-Systeme
- Andere/IOT-Systeme
- Kommunikationsverbindungen
- Räume
- Personen
- Baustein(e)
 - System-Bausteine
 - APP
 - APP.1.1 Office-Produkte
 - INF
 - INF.7 Büroarbeitsplatz
 - NET

Abteilungsserver

Kürzel S1

Titel Abteilungsserver

Tags

Beschreibung

Verknüpfungen

Objektbrowser

SYS.1.2.2.A3 Sichere Administration von Windows Server 2012

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

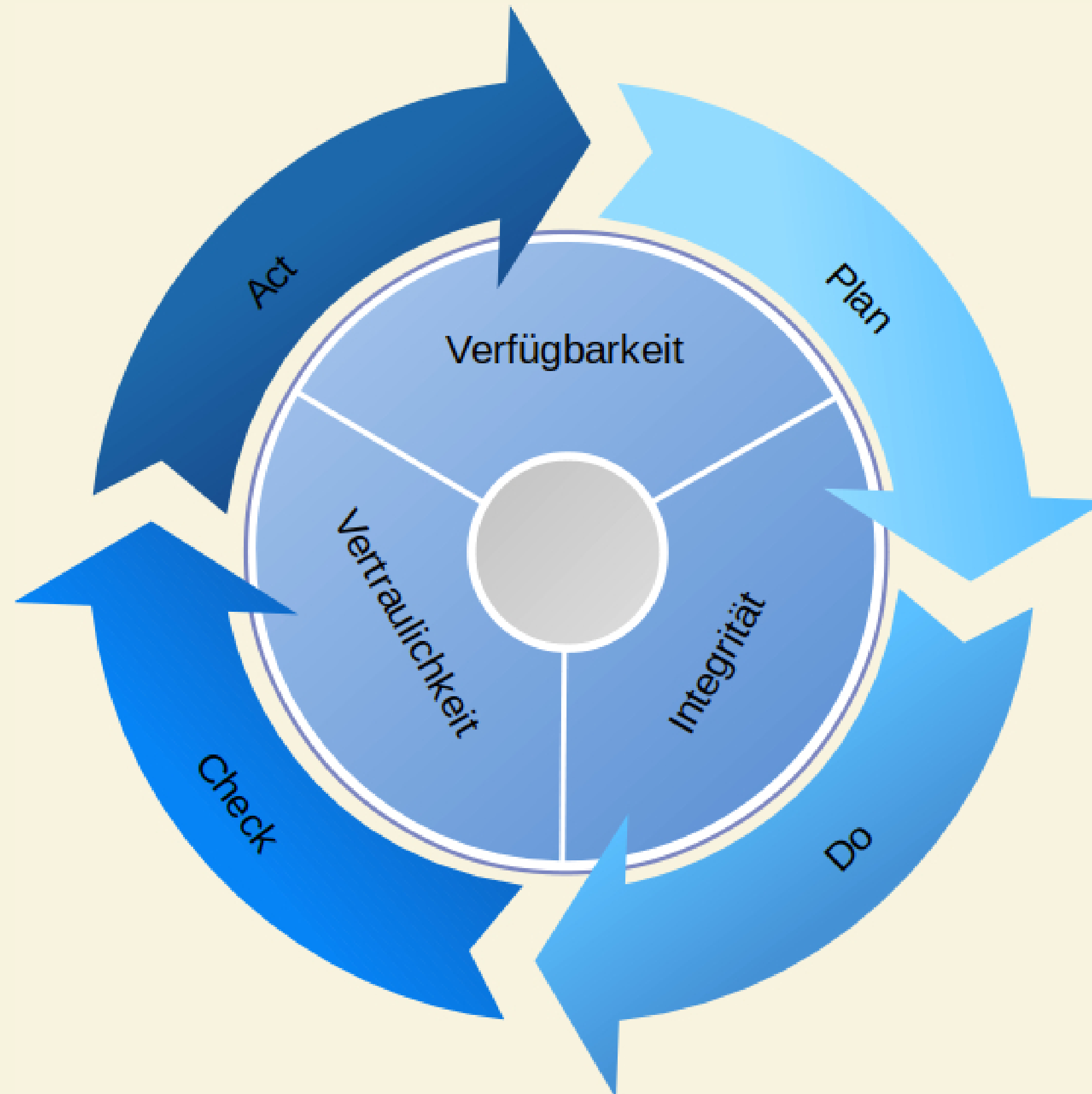
- Open Source Information Security Management System (ISMS)
- GNU General Public License
- Windows, Linux and OS X
- Demo und Kaufversion auf Hersteller Webseite
- Einzelplatz und Serverversion verfügbar
- Quellcode auf [github](#)

DEMO

OFFENE PUNKTE

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

YOU BETTER GET USED TO IT



ZUSAMMENFASSUNG

- Informationssicherheit ist finanziell bewertbar
- Fahrplan und Basis Knowhow wird kostenlos bereitgestellt
- Aufrechterhaltung der Informationssicherheit ist ein neues geschäftsrelevantes Aufgabenfeld

DIE DSGVO ALS CHANCE NUTZEN

EIN FAHRPLAN FÜR EIN MEHR AN INFORMATIONSSICHERHEIT IN KLEINEN SCHRITTEN

hagen.bauer@rusticus-consulting.de