Datenschutzmanagement im Zeichen der DS-GVO mit ISIS12

BSP-SECURITY

IT-Sicherheit am Donaustrand Regensburg

Die EU-Datenschutzgrundverordnung (DS-GVO) und ihre Umsetzung im Unternehmen

06.07.2017

Michael Gruber

Fachbeirat Datenschutz (Bayerischer IT-Sicherheitscluster e.V.)
ISIS12 Initiator und Architekt (ISMS-Standard für KMU)

Seit 30 Jahren im IT Bereich tätig (UNIX, LAN/WAN, IT-Security)
Seit 18 Jahren Berater im Bereich IT-Compliance

- **Datenschutz (Externer Datenschutzbeauftragter, Coach und Auditor)**
- **Informationssicherheit (ISO/IEC 27001, ISIS12, BSI IT-Grundschutz)**

Mitgliedschaften:

- **Bayerischer IT- Sicherheitscluster e.V.**
- **Berufsverband der Datenschutzbeauftragten Deutschlands e.V.**
- **Gesellschaft für Datenschutz und Datensicherheit e.V.**
- **Mitglied BSI Cyber-Allianz**
- **…**

BSP-SECURITY

Michael Gruber

Senior Consultant
Datenschutz und Informationssicherheit

ISIS12 Netzwerkpartner
Fachbeirat Bayerischer IT-Security Cluster e.V.

Tel: +49 (0)941 60 48 89-8 64
Fax: +49 (0)941 60 48 89-8 66
Mobil: +49 (0)152 32 01 04 95

BSP-SECURITY
Franz-Mayer-Str. 1
D-93053 Regensburg

E-Mail: michael.gruber@bsp-security.de
www.bsp-security.de

BSP-SECURITY

Fragen

- **Kennen Sie die DS-GVO?**
- **Kennen Sie das DSAnpUG-EU?**
- **Wissen Sie was ein ISMS ist?**
- **Kennen Sie ISIS12?**
- **Haben Sie ein ISMS etabliert?**

- **Für die Profis - bestimmen Sie:**
  Anzahl Artikel DS-GVO + Anzahl Erwägungsgründe DS-GVO + Anzahl Paragraphen DSAnpUG-EU

- **Lösung**
- **diesmal nicht 42!**

BSP-SECURITY

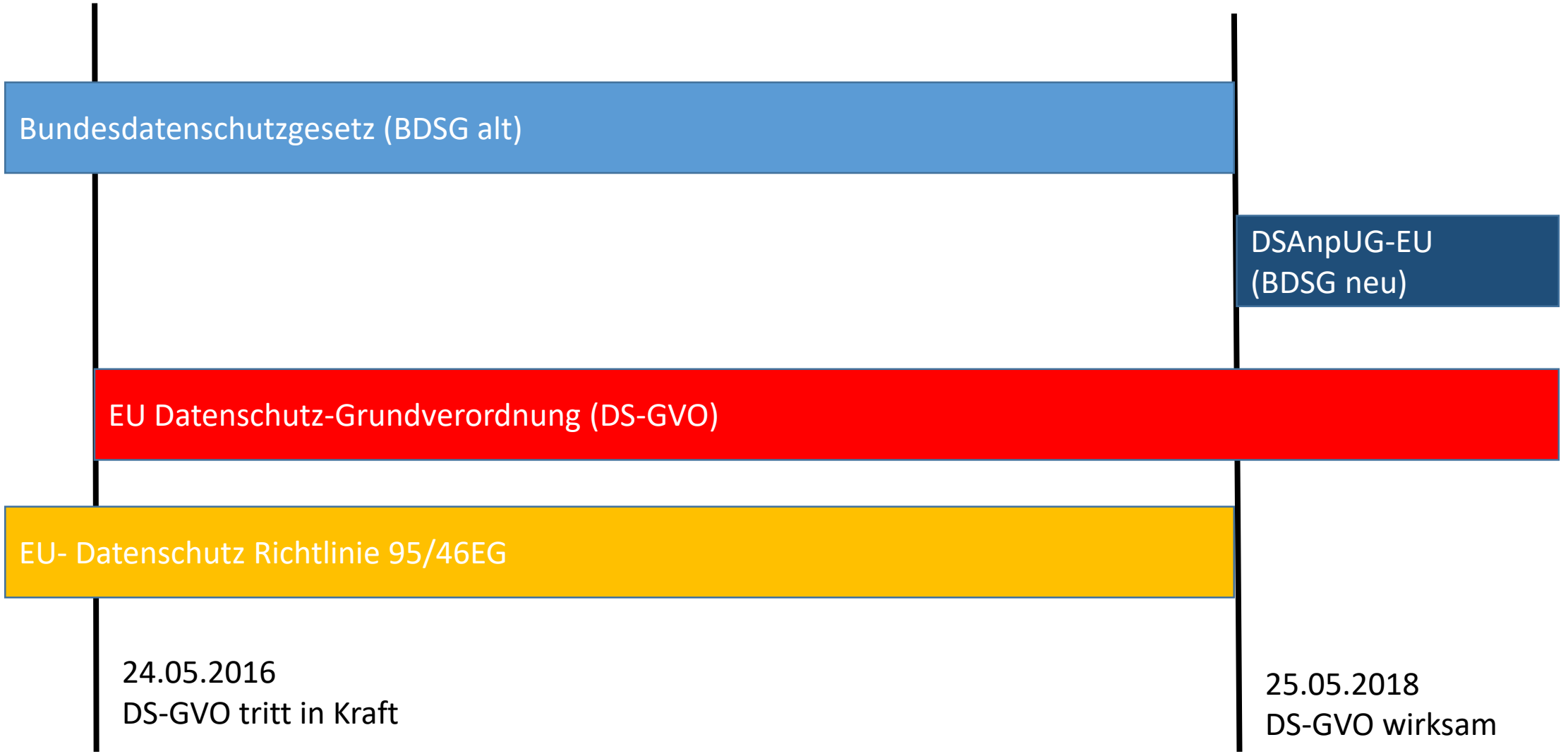
Was?

0 Ziel

~~Was?~~

Wie!

1 Datenschutz 2016-2018



BSP-SECURITY

2 Datenschutz 2018

25.05.2018
Gesetze werden wirksam

EU Datenschutz-Grundverordnung (DS-GVO)

DSAnpUG-EU* (BDSG neu)

* Gesetze zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

BSP-SECURITY

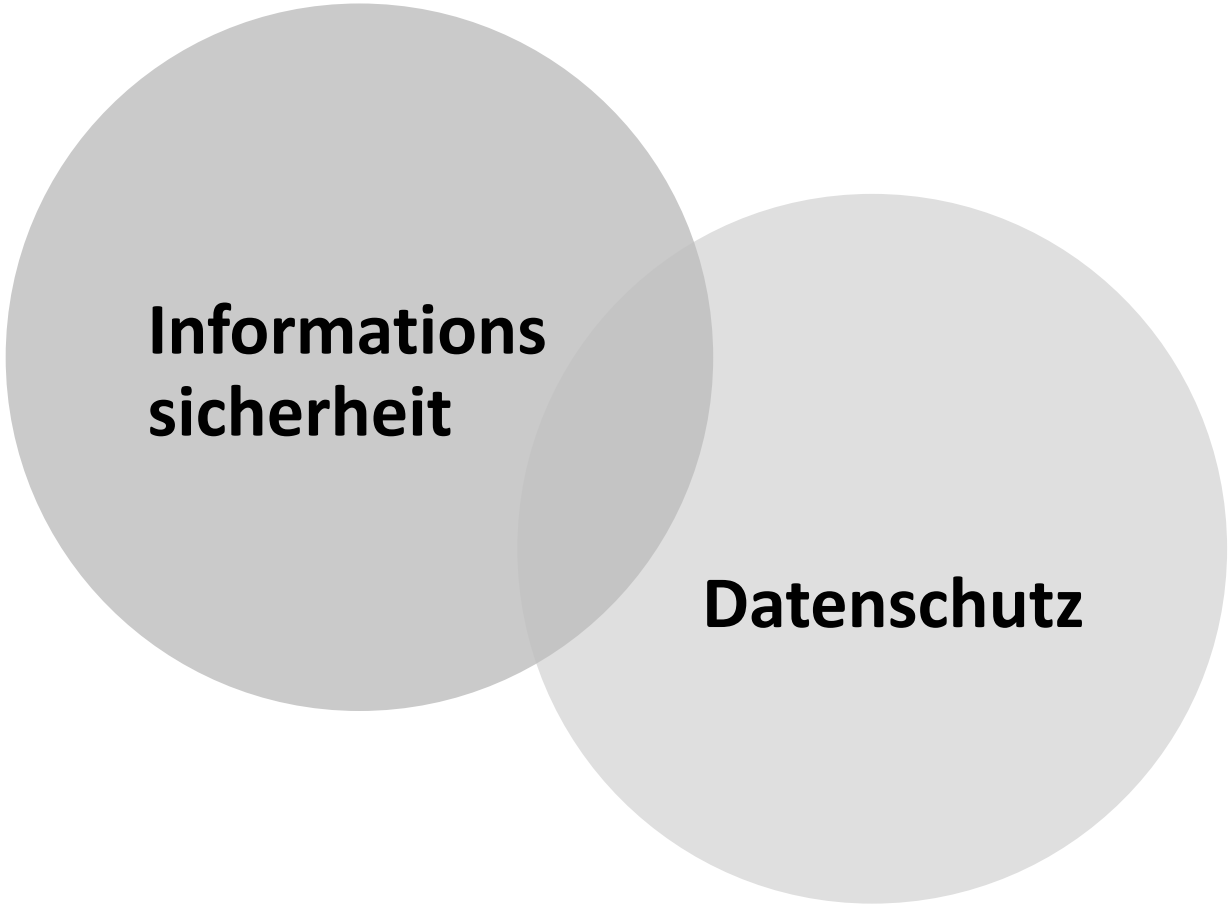
3 DS-GVO – was ist/wird neu?

- Verordnung ersetzt nationale Gesetze 27(28) nationale Regelungen
- Aber über 50 mögliche Öffnungsklauseln für nationale Regelungen, in Deutschland: DSAnpUG-EU
- Bußgelder: bis maximal 20 Millionen € oder 4% vom Konzern Jahresweltumsatz
- Rechenschaftspflicht (Accountability)
- Dokumentationspflicht
- Informationspflichten und Transparenzverpflichtung
- Risikoanalyse und Datenschutz-Folgenabschätzung
- Privacy by Design (by Default)

BSP-SECURITY

4 Datenschutz trifft Informationssicherheit

2017



BSP-SECURITY

we make security simple.

4 Datenschutz trifft Informationssicherheit

2018

BSP-SECURITY

we make security simple.

5 DS-GVO und Informationssicherheit

- **Die TOMs des BDSG (§ 9 Anlage BDSG) werden erwachsen**
- **Informationssicherheit und Datenschutz wachsen durch die DS-GVO eng zusammen**
- **Die TOMs werden zur Sicherheitskonzeption**
- **Grundwerte**
  - Vertraulichkeit, Integrität und Verfügbarkeit (ISMS, DS-GVO) +
  - Belastbarkeit (DS-GVO)

BSP-SECURITY

6 Informationssicherheit - ISMS

- **Informationssicherheit = IT-Security + Prozesse + Regelungen + Mitarbeiter**
- **Wie kann Informationssicherheit gewährleistet werden?**
  - Es muss ein Sicherheitsprozess initiiert werden (top down)
  - Technik und Organisation muss einbezogen werden
  - Prozesse müssen angepasst werden
  - Ständige Anpassung der Sicherheitsmaßnahmen
  - PDCA (Plan-Do-Check-ACT)
  - Managmentsystem
  - Summe: **ISMS**!

- **Diät vs. Ernährungsumstellung**
- **ISMS entspricht der Ernährungsumstellung**

BSP-SECURITY

7 ISIS12

- ISIS12 = Informations-SIcherheitsmanagementSystem in 12 Schritten
- Entwickelt vom „Netzwerk Informationssicherheit für den Mittelstand“ (NIM) innerhalb des Bayerischen IT-Sicherheitsclusters e.V.
- „Einfaches“ Vorgehensmodell zur Einführung eines ISMS
- Für KMU – später für Kommunen, Universitäten, NGO …
- Verständlich beschriebener 12-stufiger Prozess (inkl. Software)
- ISMS wird mit IT-Service Management verknüpft
- Migration zur ISO/IEC 27001 ist „organisch“ möglich (Pilot aktuell)
- Unternehmen wurde 2016 mit ISIS12 SOX-compliant zertifiziert
- DS-GVO kann mit ISIS12 realisiert werden

BSP-SECURITY

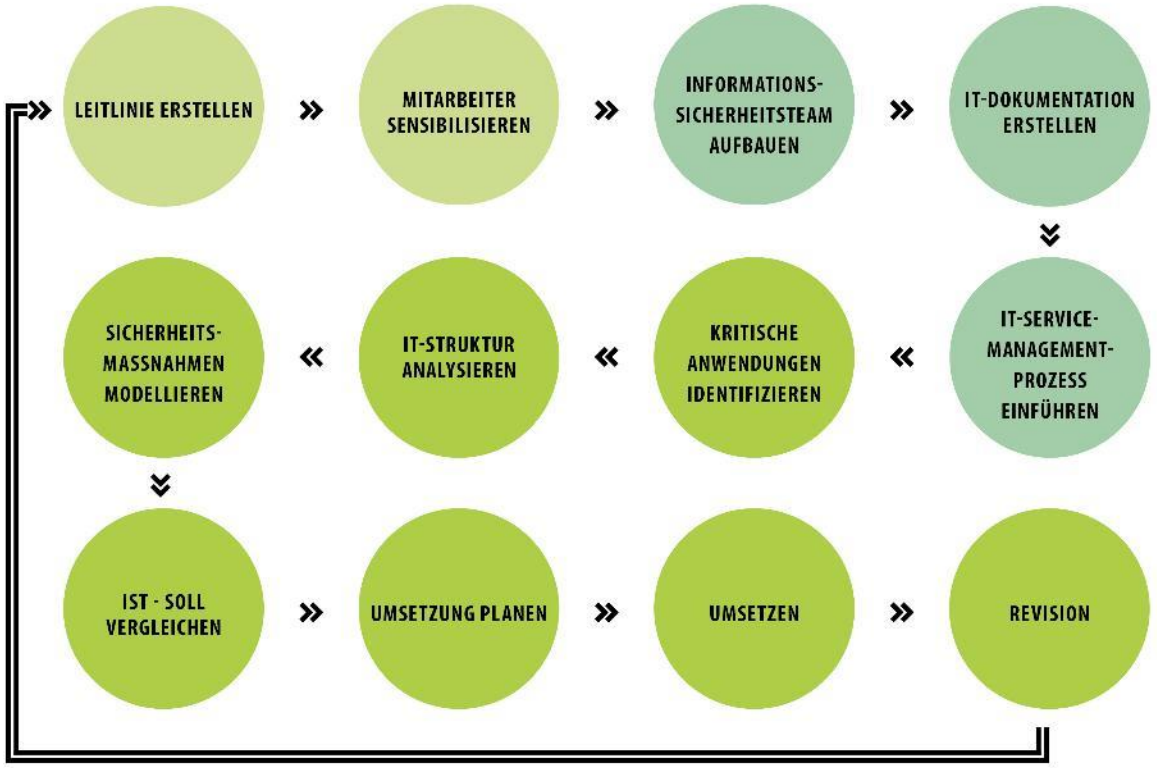
7 ISIS12

Architektur

Initialisierungsphase
Schritte 1-2

Aufbau- und
Ablauforganisation
Schritte 3-5

Entwicklung und
Umsetzung ISIS12
Konzept
Schritte 6-12



BSP-SECURITY

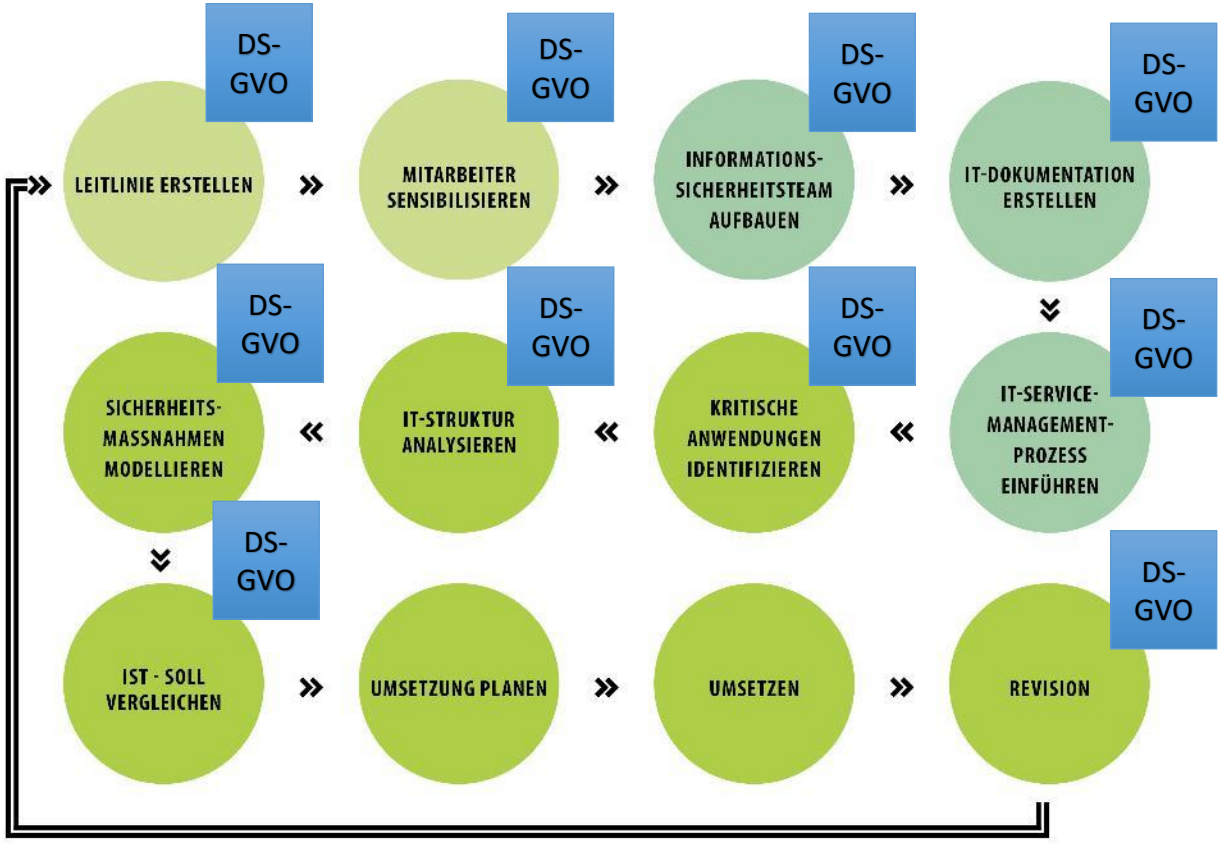
7 ISIS12 und DS-GVO

Architektur Erweiterung

Initialisierungsphase
Schritte 1-2

Aufbau- und Ablauforganisation
Schritte 3-5

Entwicklung und Umsetzung ISIS12 Konzept
Schritte 6-12



BSP-SECURITY

we make security simple.

8 Matching DS-GVO - ISIS12

ISIS12 Schritt 6: Kritische Anwendungen identifizieren

Anwendung		Schutzbedarfsfeststellung			
#	Bezeichnung	personenbezogene Daten ja / Nein	Grundwert	Schutzbedarf	Begründung
A1	Personaldaten-verarbeitung	ja	Vertraulichkeit	B	
			Integrität	A	
			Verfügbarkeit	A	
			Besonders kritische Zeiten:		
MTA	MTD	24 h		12 h	
Fachverantwortlich:		Frau Dagmar Huber (AL Personal)			
Interviewer:		Herr Franz Muster (ISB)			
Datum:		23.03.2011			
Unterschrift:		XXX			

BSP-SECURITY

we make security simple.

8 Matching DS-GVO - ISIS12

ISIS12 Schritt 6: Kritische Anwendungen identifizieren

+ Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

- **Kernstück des Datenschutz-Managements**
- **Rechenschaftspflicht (Accountability)**
- **Allgemeine Angaben**
- **Rechtsgrundlage der Verarbeitung**
- **Informationspflichten**
- **Löschfristen**
- **…**

BSP-SECURITY

8 Matching DS-GVO - ISIS12

ISIS12 Schritt 6: Kritische Anwendungen identifizieren + Risikoanalyse (Art. 32 DS-GVO)

2.6.1.2 Sicherheit der Verarbeitung - Risikoanalyse (DFA) (Art. 32)

Für Verarbeitungen in denen pbD verarbeitet werden ist die Sicherheit der Verarbeitung sicherzustellen. Hierzu wird eine Risikoanalyse durchgeführt, die teilweise auf Ergebnisse des ISIS12 Vorgehensmodells zurückgreift. Für die Einschätzung der Risiken können etwa die „G0 Elementaren Gefährdungen" (n=46) des BSI verwendet werden.

Wahrscheinlichkeiten des Eintritts eines Ereignisses:

Selten	1	Ereignis könnte nach heutigem Kenntnisstand nicht öfter als alle 10 Jahre einmal eintreten.
Oft	2	Ereignis könnte nach heutigem Kenntnisstand nicht öfter als alle 3 - 10 Jahre einmal eintreten.
Sehr oft	3	Ereignis könnte nach heutigem Kenntnisstand nicht öfter als innerhalb von 3 Jahren einmal eintreten.

Die Schadenshöhe bzw. die Auswirkung eines Ereignisses wurde bereits im Rahmen der organisations-spezifischen Schutzbedarfsfeststellung vorgenommen und dokumentiert. Diese Ergebnisse werden für die RA herangezogen und gewichtet kodiert:

Kummulierter Schutzbedarf (A= 1, B=2 oder 3, C= 3 oder 6)																										
Integrität 1 3 6	1									3									6							
Vertraulichkeit 1 3 6	1			3			6			1			3			6			1			3			6	
Verfügbarkeit 1 2 3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Summe SB	**1**	**2**	**3**	**3**	**6**	**9**	**6**	**12**	**18**	**3**	**6**	**9**	**9**	**12**	**27**	**18**	**36**	**48**	**6**	**12**	**18**	**18**	**24**	**54**	**36**	**72**	**96**

Die die Risikoklassen ergeben sich nach folgender Tabelle:

Risikoklassen				
Häufigkeit		Selten	Oft	Sehr oft
Kumulierter Schutzbedarf	1-6			
	9-36			
	48-96			

Tolerierbar
Beträchtlich
Katastrophal

BSP-SECURITY

we make security simple.

8 Matching DS-GVO - ISIS12

Schritt 1:	**Erweiterung der Sicherheitsleitlinie → Datenschutzrichtlinie**
Schritt 2:	**Datengeheimnis und Schulung Mitarbeiter** **§ 53 (DSAnpUG-EU)**
Schritt 3:	**Datenschutzbeauftragter** **Art. 37, 38, 39 … (DS-GVO)** **§§ 5, 7, 38 … (DSAnpUG-EU)**
Schritt 4:	**…**
Schritt 5:	**Datenschutzprozesse** **Art. 15, 16, 17, 18, 19, 20, 21, 22, 33, 34 … (DS-GVO)** **§§ 29, 34, 35 … (DSAnpUG-EU)**
Schritt 6:	**Art. 6, 7, 8, 9, 24, 28, 30, 32, 35, 44 … (DS-GVO)**
Schritt 7:	**Art. 32 (DS-GVO)**
…	**…**
Schritt 12:	**Zertifizierung** **Art. 42 (DS-GVO)**

BSP-SECURITY

Fazit

- ISIS12 ist ein etablierter Standard für Informationssicherheit
- ISIS12 erfüllt als Vorgehensmodell mit der DS-GVO Erweiterung die Erfordernisse der DS-GVO
- ISIS12-Zertifizierung ist möglich
- ISIS12 Zertifizierungsstandard ist transparent und öffentlich
- ISIS12 ist speziell für KMU entwickelt worden
- ISIS12 wird vom IT-Planungsrat für Kommunen empfohlen
- ISIS12 als integriertes Managementsystem
  - Informationssicherheit
  - Datenschutz
  - SOX

BSP-SECURITY