Mit ISIS12 zur DS-GVO Compliance

IT-Sicherheit am Donaustrand Regensburg

21.06.2018

Michael Gruber

IT-Compliance Berater

- Datenschutz (Coaching, Ausbildung, Audits, Externer DSB)

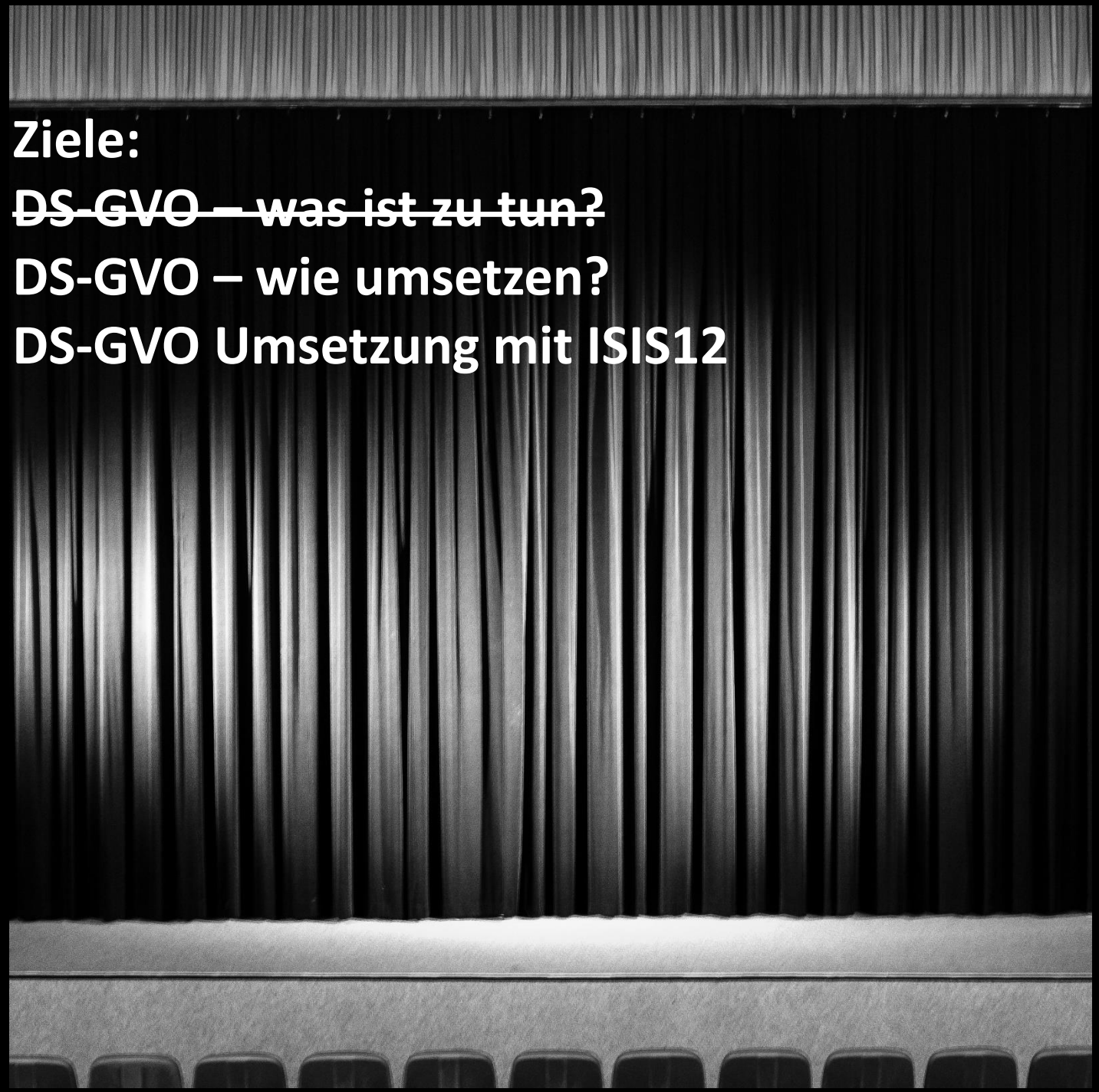
- Informationssicherheit (ISIS12 und ISO/IEC 27001)

Fachbeirat Datenschutz im Bayerischen IT- Sicherheitscluster e.V.

ISIS12 Initiator und Architekt

BSP-SECURITY

we make security simple.



Ziele:

~~DS-GVO – was ist zu tun?~~

DS-GVO – wie umsetzen?

DS-GVO Umsetzung mit ISIS12

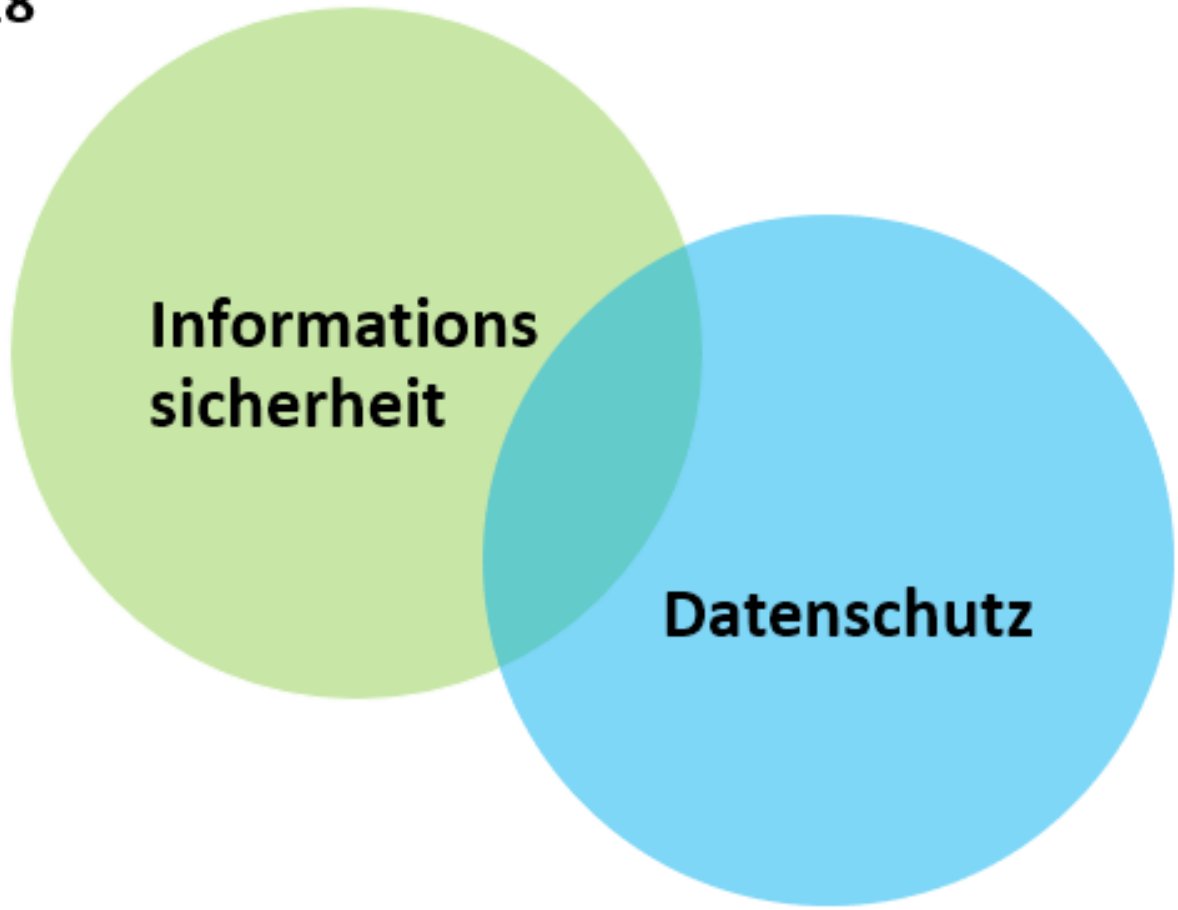
1 Informations-sicherheit trifft Datenschutz

Datenschutz und Informationssicherheit: Gemeinsamkeiten?

Schutz – Verteidigung von Grundwerten

1 Informationssicherheit trifft Datenschutz

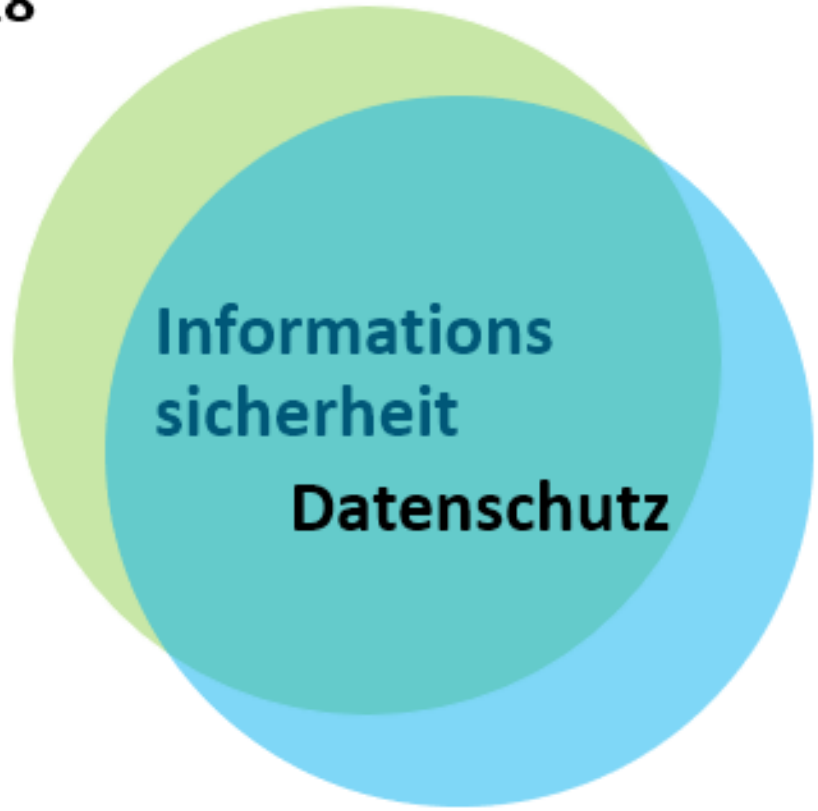
bis zum 24.05.2018



BSP-SECURITY

1 Informationssicherheit trifft Datenschutz

ab dem 25.05.2018



BSP-SECURITY

1 Informationssicherheit trifft Datenschutz

ab dem 25.05.2018

BSP-SECURITY

we make security simple.

1 Informationssicherheit trifft Datenschutz

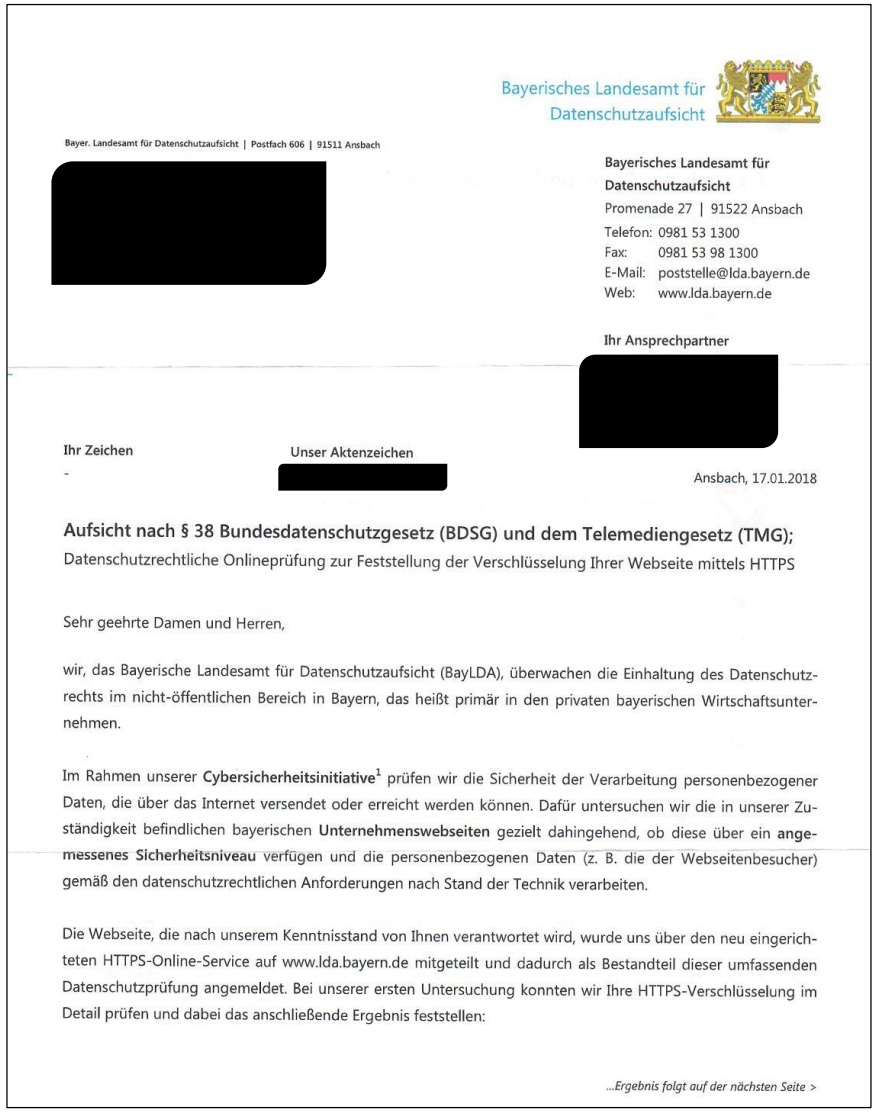
- **Grundwerte (ISIS12 und DS-GVO*)**
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit (resilience)*

- **Sinnvolle und notwendige Verknüpfung von Informationssicherheit, Organisation und Recht**
- **Spiegelt sich auch in den aktuellen personellen Besetzungen der Datenschutz-Aufsichtsbehörden wieder:**
- **z.B. Frau Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein Diplom-Informatikerin**

BSP-SECURITY

1 Informationssicherheit trifft Datenschutz

Beispiel aus der Praxis:
Post vom BayLDA



Bayerisches Landesamt für Datenschutzaufsicht

Bayer. Landesamt für Datenschutzaufsicht | Postfach 606 | 91511 Ansbach

[redacted]

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 | 91522 Ansbach
Telefon: 0981 53 1300
Fax: 0981 53 98 1300
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ihr Ansprechpartner
[redacted]

Ihr Zeichen
-

Unser Aktenzeichen
[redacted]

Ansbach, 17.01.2018

Aufsicht nach § 38 Bundesdatenschutzgesetz (BDSG) und dem Telemediengesetz (TMG);
Datenschutzrechtliche Onlineprüfung zur Feststellung der Verschlüsselung Ihrer Webseite mittels HTTPS

Sehr geehrte Damen und Herren,

wir, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), überwachen die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, das heißt primär in den privaten bayerischen Wirtschaftsunternehmen.

Im Rahmen unserer **Cybersicherheitsinitiative**[1] prüfen wir die Sicherheit der Verarbeitung personenbezogener Daten, die über das Internet versendet oder erreicht werden können. Dafür untersuchen wir die in unserer Zuständigkeit befindlichen bayerischen **Unternehmenswebseiten** gezielt dahingehend, ob diese über ein **angemessenes Sicherheitsniveau** verfügen und die personenbezogenen Daten (z. B. die der Webseitenbesucher) gemäß den datenschutzrechtlichen Anforderungen nach Stand der Technik verarbeiten.

Die Webseite, die nach unserem Kenntnisstand von Ihnen verantwortet wird, wurde uns über den neu eingerichteten HTTPS-Online-Service auf www.lda.bayern.de mitgeteilt und dadurch als Bestandteil dieser umfassenden Datenschutzprüfung angemeldet. Bei unserer ersten Untersuchung konnten wir Ihre HTTPS-Verschlüsselung im Detail prüfen und dabei das anschließende Ergebnis feststellen:

...Ergebnis folgt auf der nächsten Seite >

HTTPS-Check

Ergebnis der Onlineprüfung zur Verschlüsselung Ihrer Webseite

Geprüfte Webseite:
[redacted]

Datum der Prüfung:
09.01.2018

Geprüft durch:
Bayerisches Landesamt für Datenschutzaufsicht

wirksame HTTPS-Verschlüsselung vorhanden

- ✓ Einsatz einer HTTPS-Verschlüsselung
- ✓ Kein Einsatz veralteter Verschlüsselungsprotokolle (SSL2, SSL3)
- ✓ TLS 1.2 als Standardprotokoll
- ✓ Priore Verwendung von Perfect Forward Secrecy (PFS)
- ✓ Geeignete Schlüssellänge des SSL-Zertifikats
- ✓ Keine SSL-Zertifikate mit SHA-1
- ✓ Keine unsicheren Kryptoalgorithmen (z. B. RC4, Export-Chiffren,...)
- ✗ Verwendung von http Strict Transport Security (HSTS)
- ✓ Geeignete SSL-Zertifikate

Sobald auf Ihrer Webseite der fehlende Umsetzungspunkt nachgeholt wird, wird diese den Anforderungen des BDSG, insbesondere nach § 9 BDSG samt Anlage zu § 9 BDSG, erfüllen. Bitte informieren Sie uns schriftlich **bis spätestens zum 16.02.2018** über die erfolgte Anpassung (gerne auch durch eine E-Mail an cybersecurity@lda.bayern.de).

Mit freundlichen Grüßen,
[redacted]
Technischer Datenschutz

BSP-SECURITY

we make security simple.

2 ISMS – ISIS12

Warum schützen Sie nur Ihre personenbezogenen Daten – was ist mit Ihren Kronjuwelen?

2 ISMS – ISIS12

ISIS12 = Informations-SIcherheitsmanagementSystem in 12 Schritten

- **Entwickelt vom Bayerischen IT-Sicherheitsclusters e.V.**
- **Vorgehensmodell zur Einführung eines ISMS speziell für KMO**
- **Verständlich beschriebener 12-stufiger Prozess (inkl. Software)**
- **Ziel: Erhöhung der Informationssicherheit („Digitale Sorglosigkeit“)**
- **Migration zur ISO/IEC 27001 vorgesehen**
- **Mit ISIS12 kann DS-GVO Compliance erreicht werden**

BSP-SECURITY

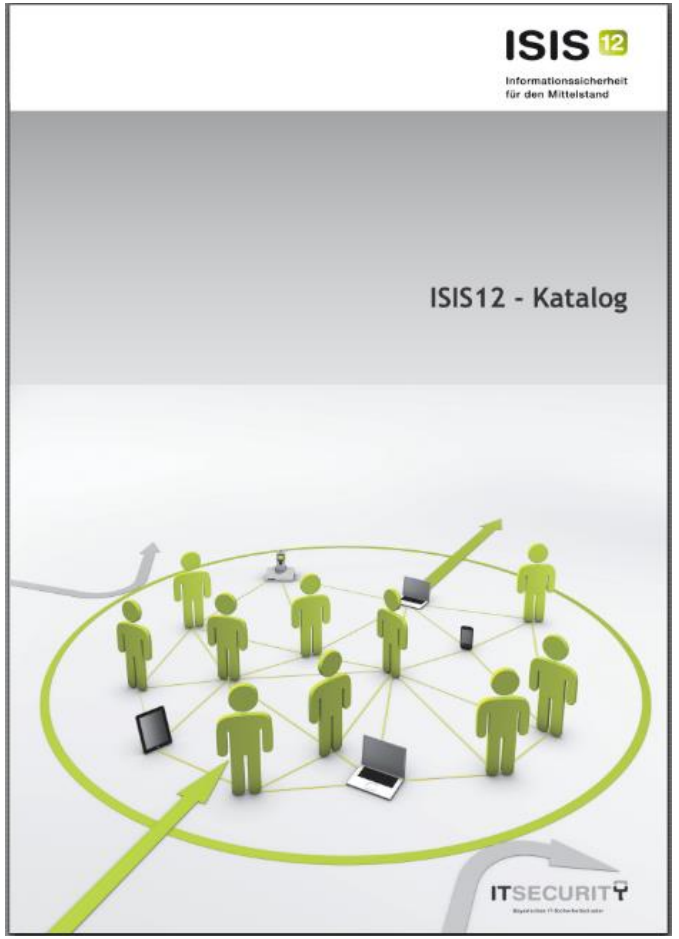
2 ISMS – ISIS12

- ISMS (InformationsSicherheitsManagementSystem):
  - Es wird ein Sicherheitsprozess initiiert (top down)
  - Technik und Organisation sind zu betrachten
  - Anpassung der Sicherheitsmaßnahmen/Prozesse (KVP)
  - PDCA (Plan-Do-Check-ACT)

- „ISMS entspricht nicht einer Diät – sondern einer Ernährungsumstellung“

BSP-SECURITY

ISIS12 – ISMS für KMO



BSP-SECURITY

3 DS-GVO mit ISIS12

3 DS-GVO mit ISIS12

Informationssicherheit in 12 Schritten

Initialisierungsphase
Schritte 1-2

Aufbau- und
Ablauforganisation
Schritte 3-5

Entwicklung und
Umsetzung ISIS12
Konzept
Schritte 6-12

BSP-SECURITY

3 DS-GVO mit ISIS12

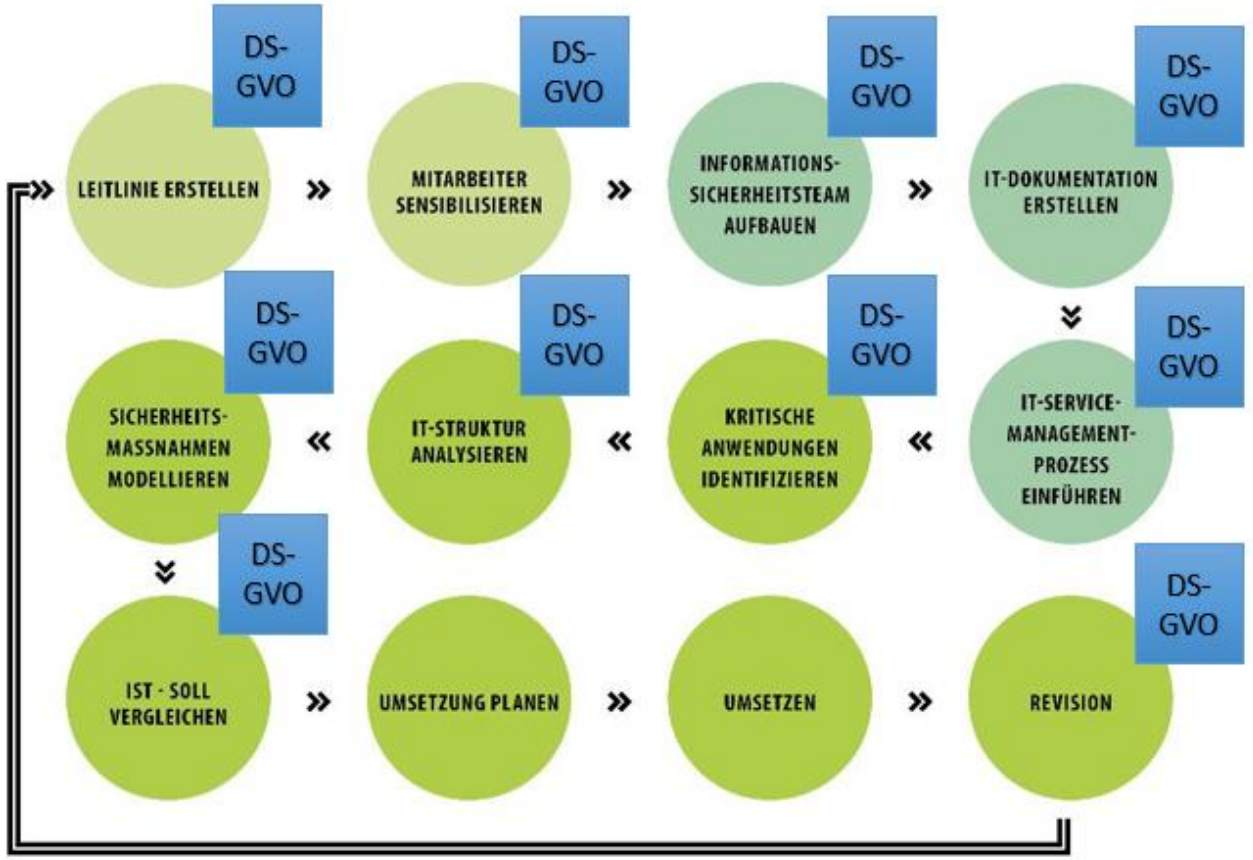
Synergie: DS-GVO/ISIS12

Architektur Erweiterung

Initialisierungsphase
Schritte 1-2

Aufbau- und Ablauforganisation
Schritte 3-5

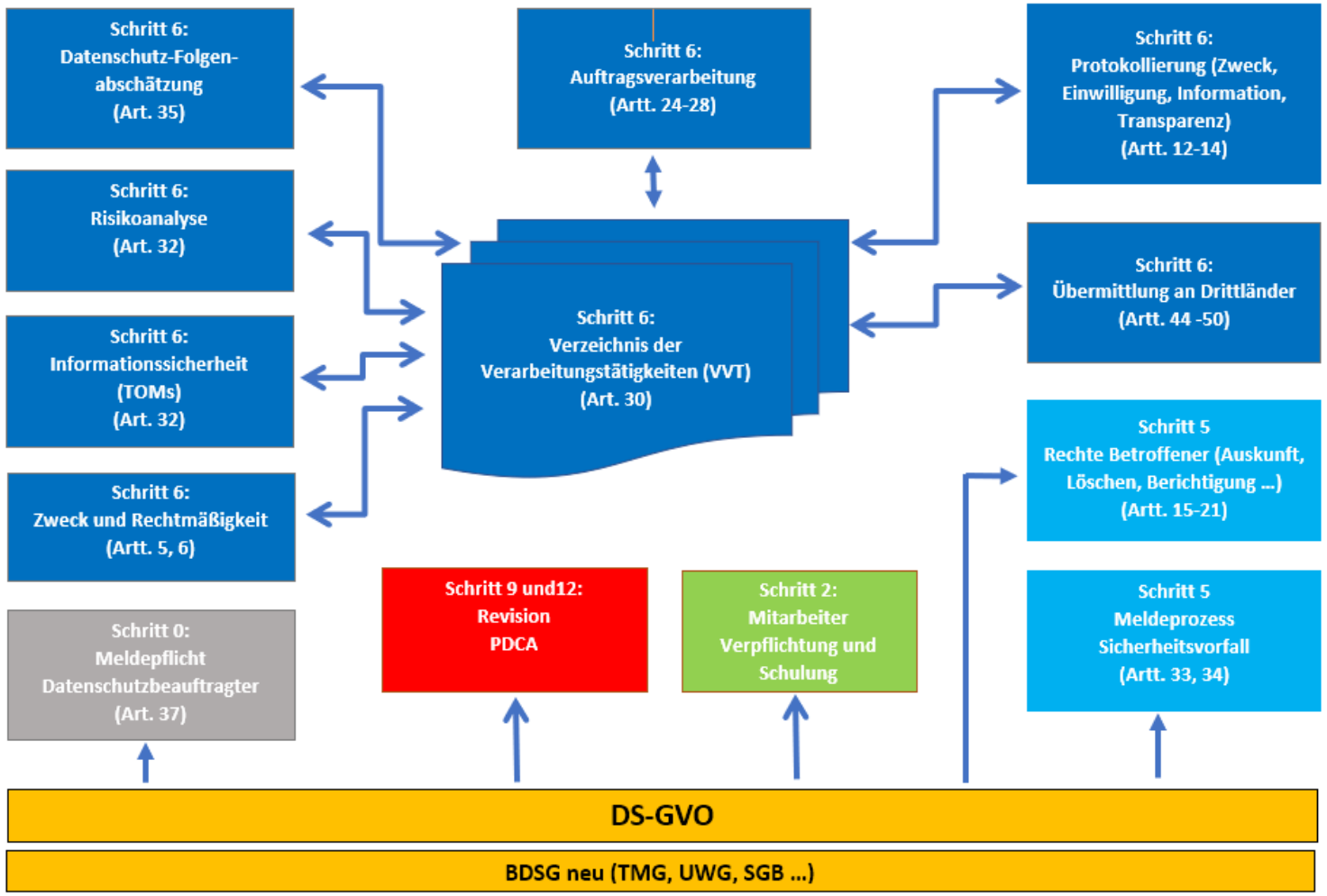
Entwicklung und Umsetzung ISIS12 Konzept
Schritte 6-12



BSP-SECURITY

3 DS-GVO mit ISIS12

Synergie: DS-GVO/ISIS12



Grundprinzipien der DS-GVO:

- Rechenschaftspflicht
- Beweisumkehr
- Belastbare Dokumentation
- Risikobasierter Ansatz
- Informations- und Transparenz
- Sicherheit der Verarbeitung
- Privacy by Design/Default
- ...

BSP-SECURITY

3 DS-GVO mit ISIS12: Schritt 4 – IT-Dokumentation erstellen

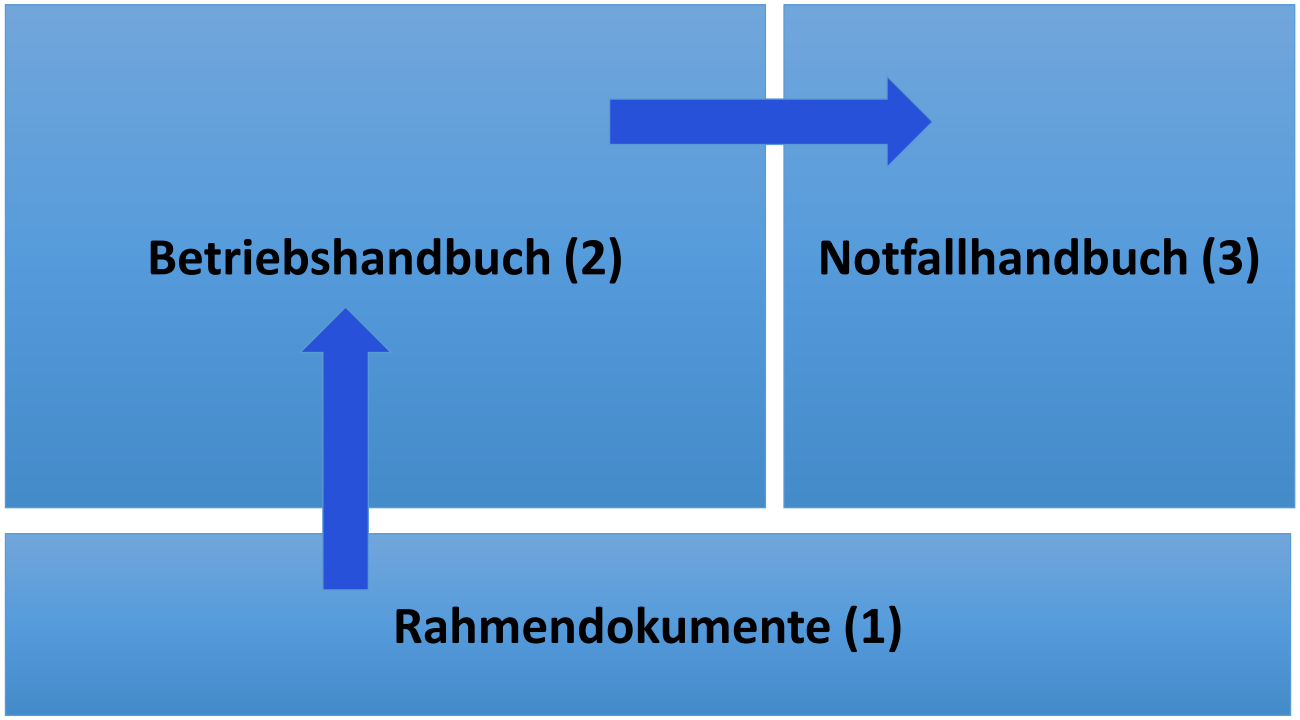
- **Eine aktuelle und strukturierte IT-Dokumentation ist eine wesentliche Voraussetzung für den Erfolg eines jeden ISMS**

- **Ziel und Aufgabe der IT-Dokumentation: Nachweis, Nachhaltigkeit, Know-How-Transfer und PDCA**

- **Die Rechenschaftspflicht der DS-GVO erfordert eine entsprechende IT-Dokumentation**

3 DS-GVO mit ISIS12: Schritt 4 – IT-Dokumentation erstellen

Logischer Aufbau der IT-Dokumentation:



Aufbau und Ablauforganisation

BSP-SECURITY

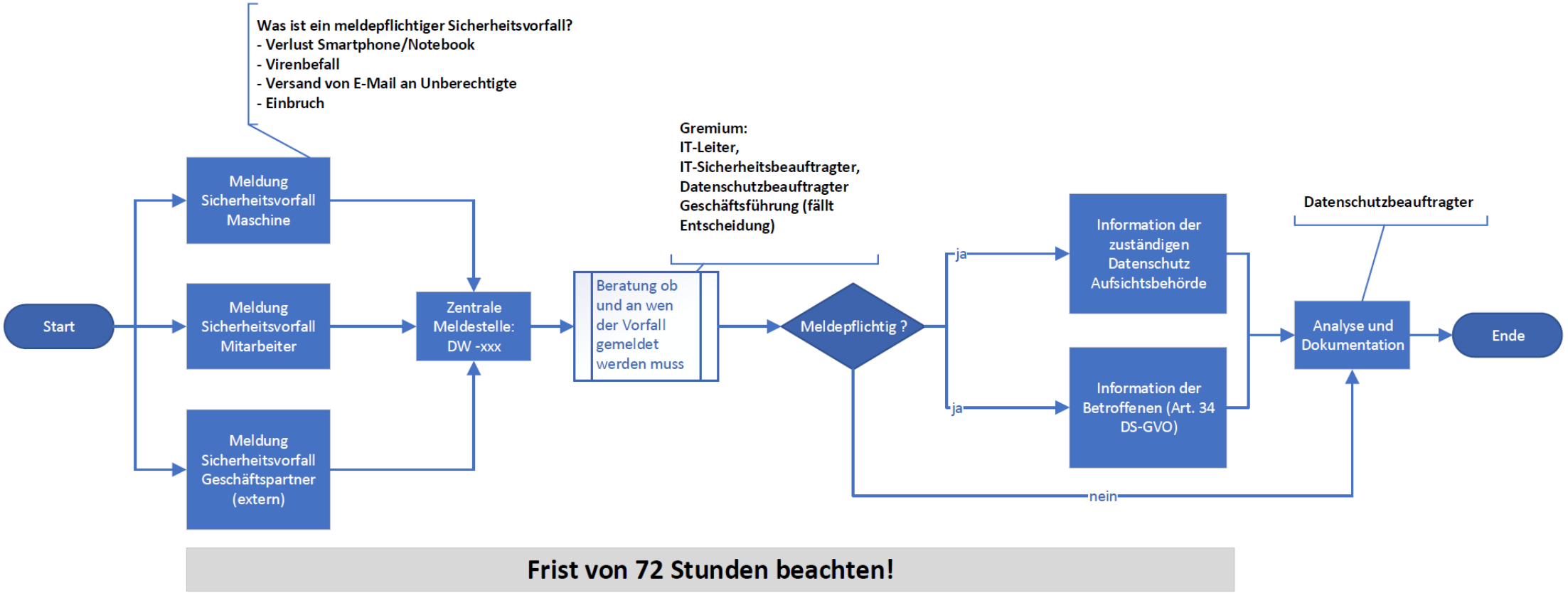
3 DS-GVO mit ISIS12: Schritt 5 – IT Servicemanagement-Prozesse

ISIS12: IT Service-Management (ITSM) mit drei Basis Prozessen

- **Wartung**
- **Änderung**
- **Störungsbeseitigung**

3 DS-GVO mit ISIS12: Schritt 5 – IT Servicemanagement-Prozesse

Muster GmbH
MA 6.1 Meldeprozess Art. 33, 34 DS-GVO (vereinfachter Musterprozess)
Autor: Michael Gruber (EDSB)
Letzte Änderung: 25.05.2018
Klassifikation: intern



BSP-SECURITY

we make security simple.

3 DS-GVO mit ISIS12: Schritt 6 – Kritische Anwendungen und DS-GVO

- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)**
- **Sicherheit der Verarbeitung TOMs (Art. 32 DS-GVO) inkl. Risikonalyse**
- **Datenschutzfolgeabschätzung (Art. 35 DS-GVO)**

Entwicklung und Umsetzung
ISIS12 Konzept

BSP-SECURITY

3 DS-GVO mit ISIS12: Schritt 6 - Kritische Anwendungen

ISIS 12 Übersicht 0 1 2 3 4 5 6 7 8 9 10 11 12

23.01.2018

Admin

Schritt 6: Kritische Applikationen identifizieren

Beschreibung

Mit **ISIS12 Schritt 6** beginnt die operative Phase des ISIS12 Vorgehensmodells.
Dabei werden wenige unternehmenskritische Anwendungen identifiziert und bewertet. Diesen werden jeweils 3 Schutzbedarfskategorien bezogen auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit zugeordnet. Aus der Schutzbedarfsfeststellung werden dann die Maximal Tolerierbare Ausfallzeit (MTA) und die Service Level Agreements (SLA) abgeleitet und im Service-Katalog dokumentiert, der über ein CMDBSoftwaretool verwaltet wird.

Kritische Applikationen | Individuelle Bausteine und Maßnahmen | Definition der Schutzbedarfskategorien | DS-GVO

Bezeichnung	Baustein/Subtyp	Beschreibung	Verantwortlicher	Vertraulichkeit	Integrität	Verfügbarkeit	PbD / MTD *
A1	Datenbankbasierende Anwendungen	Personaldatenverarbeitung	Maria Walter	B	A	B	Ja /
A2	Datenbankbasierende Anwendungen	Beihilfeabwicklung	Hans Huber	B	A	A	Ja /
A3	Datenbankbasierende Anwendungen	Reisekostenabrechnung	Hans Huber	B	A	A	Ja /
A4	Verzeichnisdienst	Benutzerauthentisierung	Hans Huber	A	B	B	Ja /
A5	Datenbankbasierende Anwendungen	Systemmanagement	Maria Walter	A	B	A	Ja /
A6	E-Mail (Server und Client)	xhange E-Mail, Terminkalender	Franz Werfel	A	A	B	Ja /
A7	Datenbankbasierende Anwendungen, Archivierung	zentrale Dokumentenverwaltung	Maria Walter	A	A	B	Ja /
A8		USB-Sticks zum Datenträgertausch	Maria Walter	A	A	A	Ja /
A9	Webserver, Nutzung von Webanwendungen	BOV-Intranet	N.N.	A	A	A	Ja /
A10	Datenbankbasierende Anwendungen	Datenbank der Grundlagendokumente	Maria Walter	A	B	B	Ja /
A11		Printservice	Maria Walter	A	A	A	Ja /

Entwicklung und Umsetzung ISIS12 Konzept

BSP-SECURITY

we make security simple.

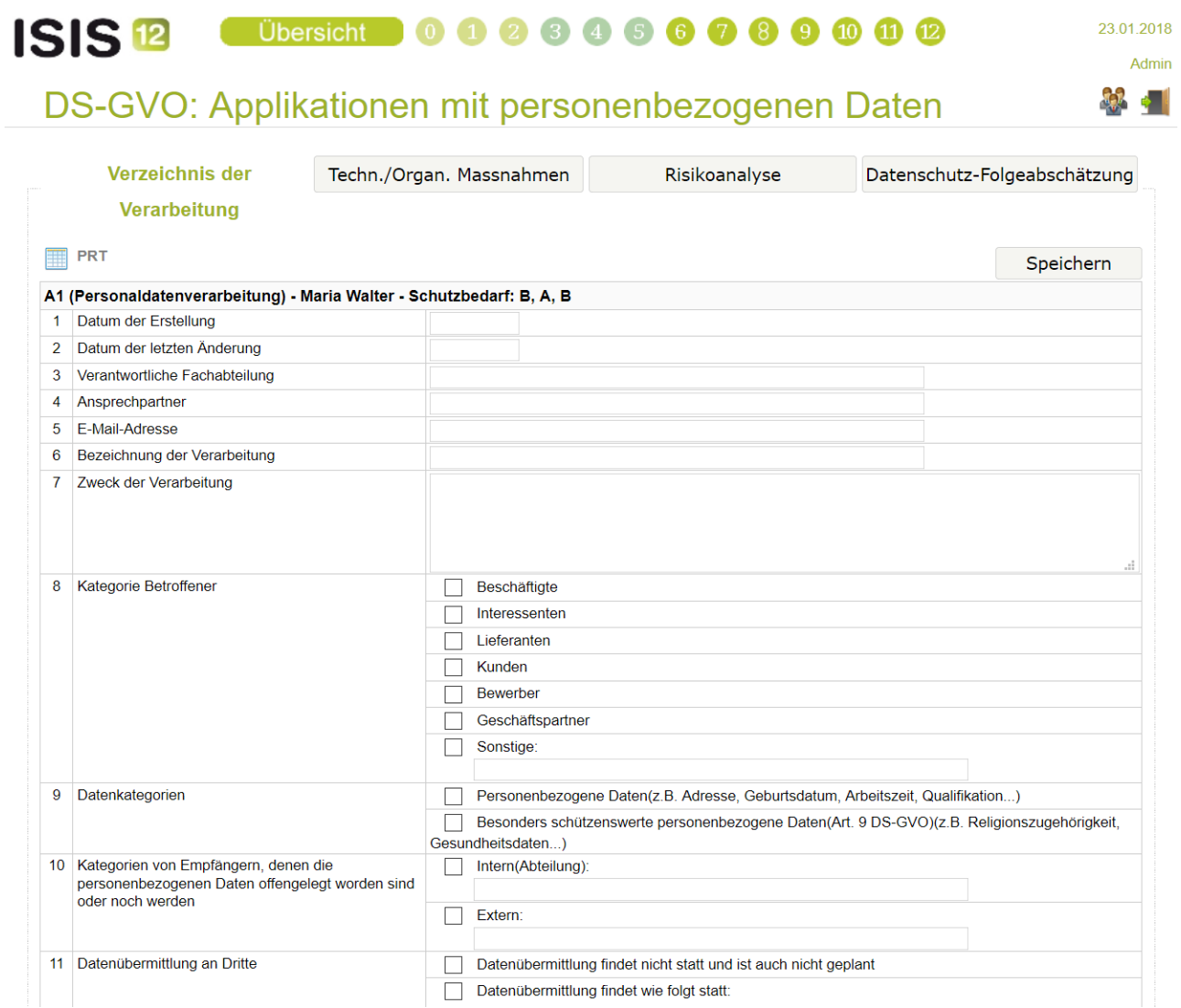
3 DS-GVO mit ISIS12: Schritt 6 - Kritische Anwendungen

Entwicklung und Umsetzung ISIS12 Konzept

BSP-SECURITY

we make security simple.

3 DS-GVO mit ISIS12: Schritt 6 – VVT (Art. 30 DS-GVO)

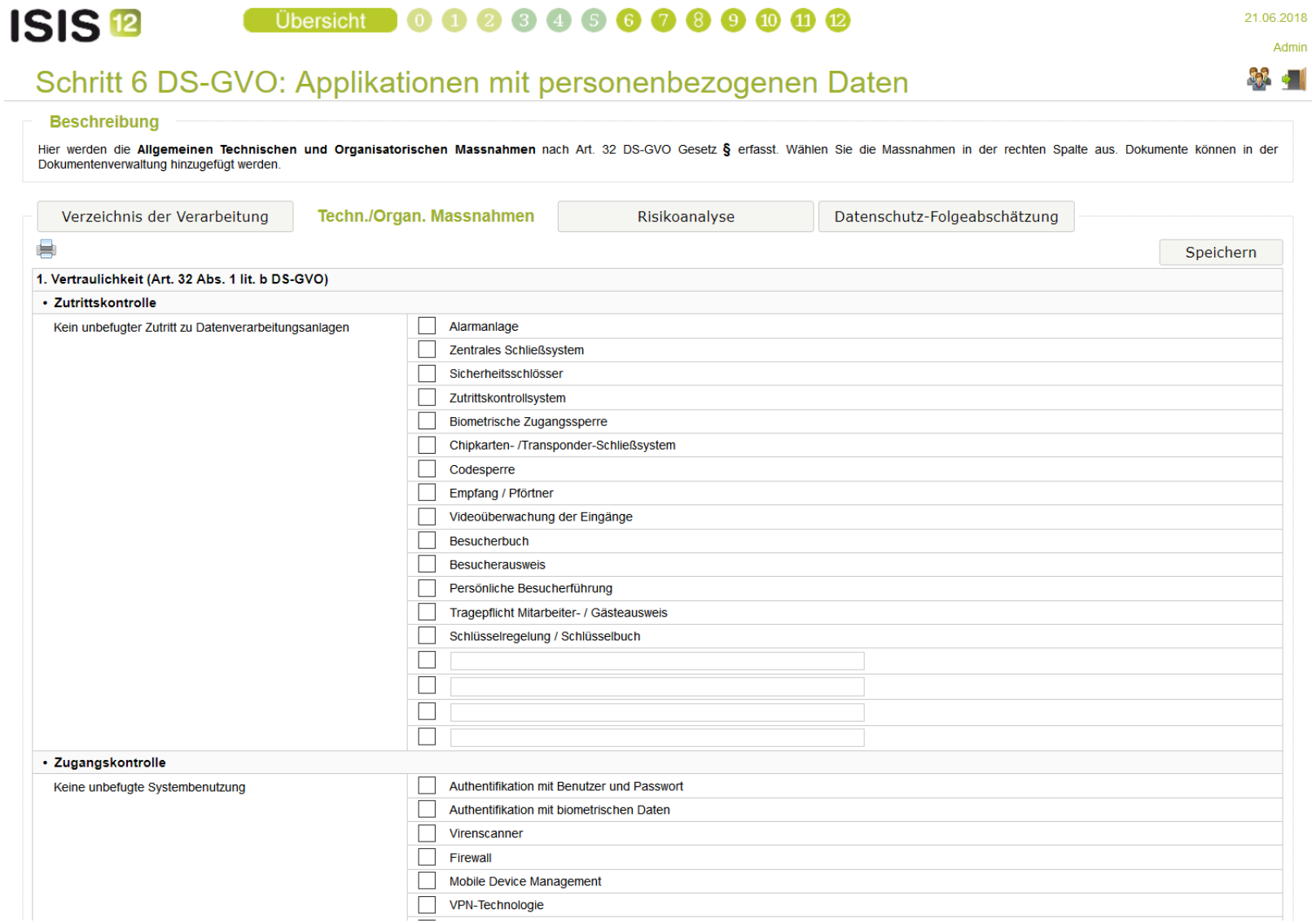


Entwicklung und Umsetzung
ISIS12 Konzept

BSP-SECURITY

we make security simple.

3 DS-GVO mit ISIS12: Schritt 6 – TOMs (Art. 32 DS-GVO)



Entwicklung und Umsetzung
ISIS12 Konzept

BSP-SECURITY

we make security simple.

3 DS-GVO mit ISIS12: Schritt 6 - Risikoanalyse

ISIS 12 Übersicht 0 1 2 3 4 5 6 7 8 9 10 11 12

24.01.2018

Admin

DS-GVO: Applikationen mit personenbezogenen Daten

Verzeichnis der Verarbeitung | Techn./Organ. Massnahmen | **Risikoanalyse** | Datenschutz-Folgeabschätzung

Speichern

A1 (Personaldatenverarbeitung) - Maria Walter

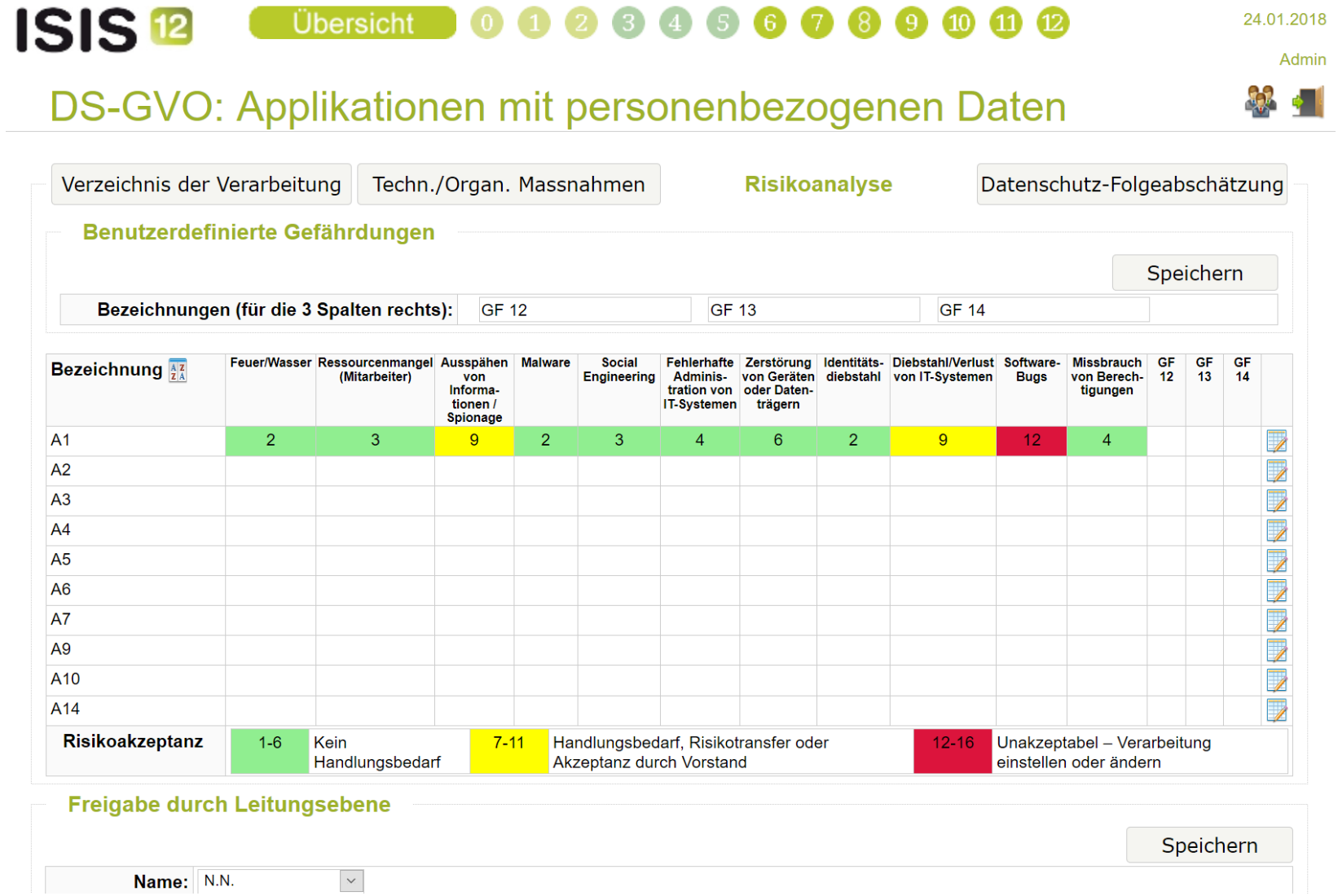
Nr.	Gefährdung	Schaden				Wahrscheinlichkeit				Bemerkung
		Niedrig	Moderat	Erheblich	Katastrophal	Möglich	Gelegentlich	Wahrscheinlich	Häufig	
01	Feuer/Wasser	○	◉	○	○	◉	○	○	○	
02	Ressourcenmangel (Mitarbeiter)	○	○	◉	○	◉	○	○	○	
03	Ausspähen von Informationen / Spionage	○	○	◉	○	○	○	◉	○	
04	Malware	◉	○	○	○	○	◉	○	○	
05	Social Engineering	○	○	◉	○	◉	○	○	○	
06	Fehlerhafte Administration von IT-Systemen	○	◉	○	○	○	◉	○	○	
07	Zerstörung von Geräten oder Datenträgern	○	◉	○	○	○	○	◉	○	
08	Identitätsdiebstahl	○	◉	○	○	◉	○	○	○	
09	Diebstahl/Verlust von IT-Systemen	○	○	◉	○	○	○	◉	○	
10	Software-Bugs	○	○	◉	○	○	○	○	◉	
11	Missbrauch von Berechtigungen	○	◉	○	○	○	◉	○	○	
12	GF 12	○	○	○	○	○	○	○	○	
13	GF 13	○	○	○	○	○	○	○	○	
14	GF 14	○	○	○	○	○	○	○	○	

Entwicklung und Umsetzung ISIS12 Konzept

BSP-SECURITY

we make security simple.

3 DS-GVO mit ISIS12: Schritt 6 - Risikoanalyse



ISIS 12 Übersicht 0 1 2 3 4 5 6 7 8 9 10 11 12

24.01.2018

Admin

DS-GVO: Applikationen mit personenbezogenen Daten

Verzeichnis der Verarbeitung | Techn./Organ. Massnahmen | **Risikoanalyse** | Datenschutz-Folgeabschätzung

Benutzerdefinierte Gefährdungen

Speichern

Bezeichnungen (für die 3 Spalten rechts): GF 12 | GF 13 | GF 14

Bezeichnung	Feuer/Wasser	Ressourcenmangel (Mitarbeiter)	Ausspähen von Informationen / Spionage	Malware	Social Engineering	Fehlerhafte Administration von IT-Systemen	Zerstörung von Geräten oder Datenträgern	Identitätsdiebstahl	Diebstahl/Verlust von IT-Systemen	Software-Bugs	Missbrauch von Berechtigungen	GF 12	GF 13	GF 14	
A1	2	3	9	2	3	4	6	2	9	12	4				
A2															
A3															
A4															
A5															
A6															
A7															
A9															
A10															
A14															

Risikoakzeptanz					
	1-6	Kein Handlungsbedarf	7-11	Handlungsbedarf, Risikotransfer oder Akzeptanz durch Vorstand	12-16	Unakzeptabel – Verarbeitung einstellen oder ändern

Freigabe durch Leitungsebene

Speichern

Name: N.N.

Entwicklung und Umsetzung ISIS12 Konzept

BSP-SECURITY

we make security simple.

3 DS-GVO mit ISIS12: Schritt 9 Datenschutz Baustein im ISIS12 Katalog

Neuer ISIS12 Datenschutz Baustein (Audit-Trail):

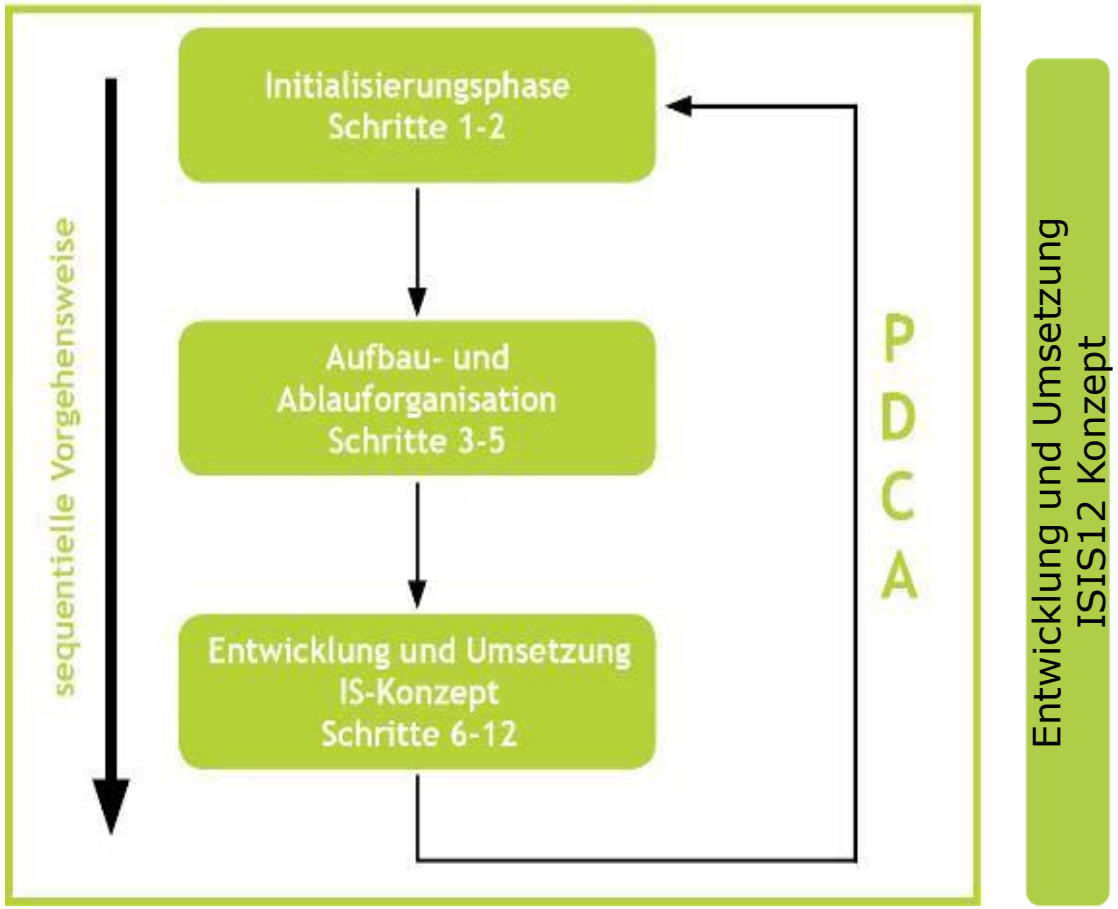
- M 2.900 Datenschutzmanagement
- M 2.901 Datenschutzbeauftragter
- M 2.902 Verzeichnis der Verarbeitungstätigkeiten
- M 2.903 Datenschutzgerechte Technikgestaltung
- M 2.904 Auftragsverarbeitung
- M 2.905 Informationspflichten
- M 2.907 Werbung - Einwilligungserklärungen
- M 2.908 Auskunft Betroffener
- M 2.909 Datenportabilität
- M 2.910 Rechtmäßigkeit der Verarbeitung
- M 2.911 Datenschutzmanagementsystem
- M 2.912 Sicherheit der Verarbeitung – Risikoanalyse
- M 2.913 Datenschutz-Folgenabschätzung
- M 2.914 Datenschutzverletzungen

Entwicklung und Umsetzung
ISIS12 Konzept

BSP-SECURITY

3 DS-GVO mit ISIS12: Schritt 12 Revision/Audit

- **PDCA-Ansatz**
- **Stetige Optimierung des IT-Sicherheitsmanagement-Systems durch weitere ISIS12-Zyklen**
- **Abruf des Revisionsplans für die Überprüfung der Maßnahmen**
- **Interne Audits (KVP)**



BSP-SECURITY

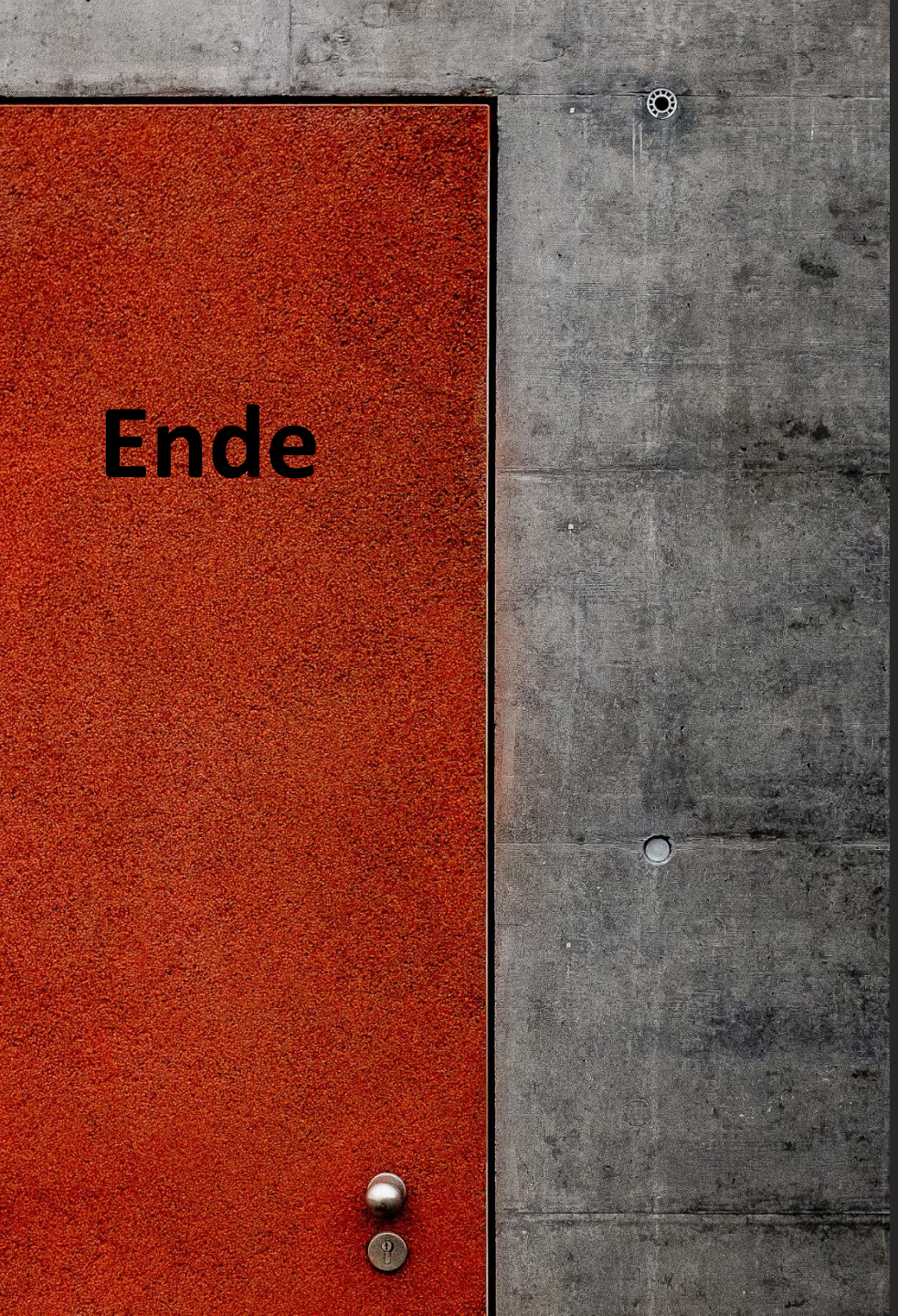
Fazit

Frage:
Ist Datenschutz/DS-GVO ohne Informationssicherheit machbar?

Antwort:
Nur schwer machbar – nicht sinnvoll!

ISIS12 ist ein Vorgehensmodell für ISMS und Datenschutzmanagement –
optimal für die KMO

Ihre Kronjuwelen werden es Ihnen danken!



BSP-SECURITY

Michael Gruber

Senior Consultant Datenschutz und Informationssicherheit

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

T +49 (0)941 46 29 09 29
M +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