



Unternehmerfrühstück:

Status quo DSGVO

Hamburg, 17. Januar 2019

Status quo DSGVO

Vorwort:

Thomas Mattheis – bakertilly

Redner:

Bernd Brodersen – outcome

Martin Beinersdorf – outcome

Andreas Höth – bakertilly

DSGVO:

- Verbindliche Rechtsgrundlage in Europa
- Identifizierter Regulierungsbedarf – die „Idee“, die dahinter steckt
- Konkrete Anforderungen und daraus resultierende Pflichten
- Verantwortlichkeiten in Unternehmen
- Einrichtung eines Datenschutz-Management-Systems

Agenda

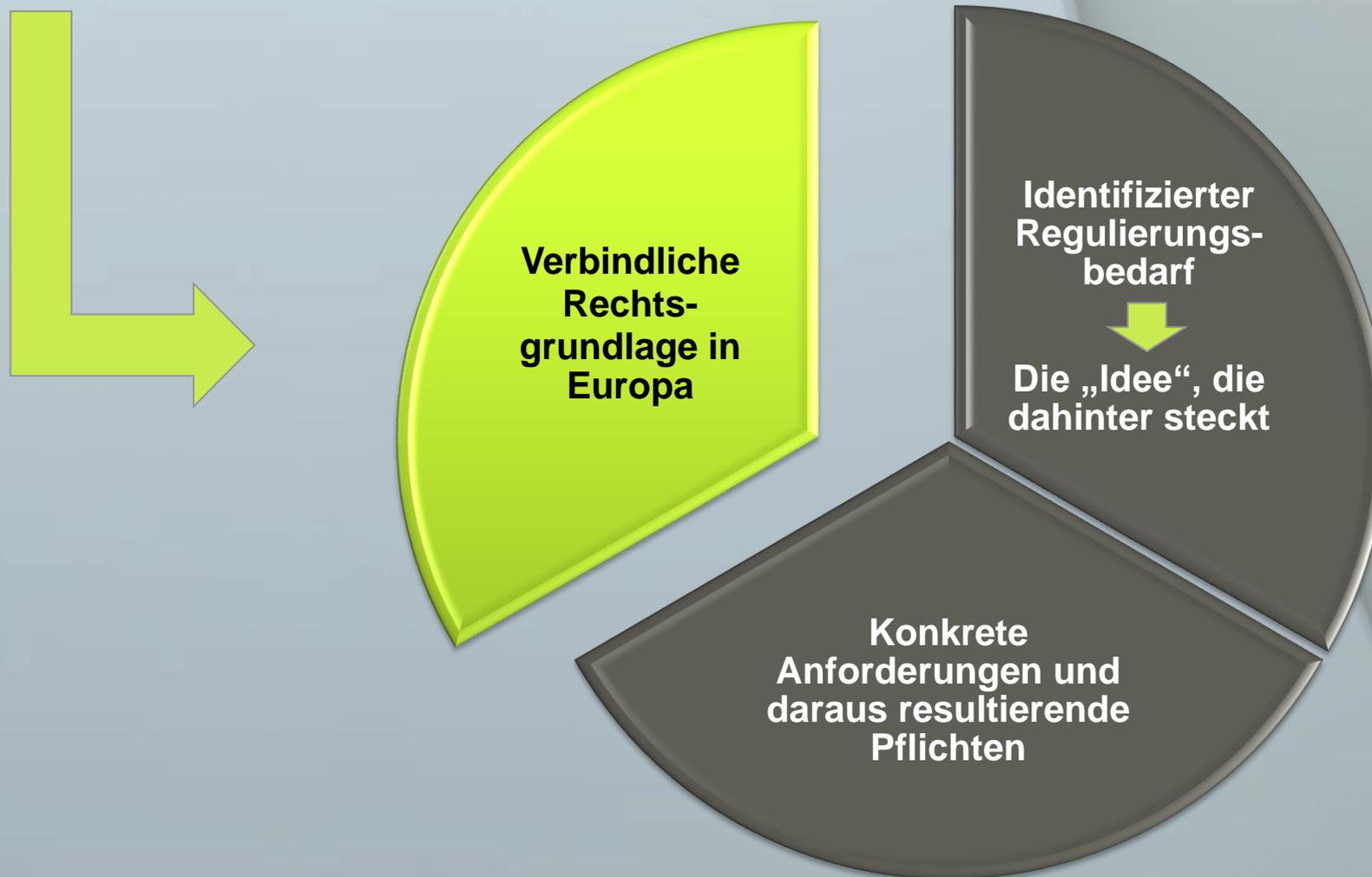
DSGVO und Bereederungstätigkeit

- Personal und Crewing: Umfangreicher Datenaustausch

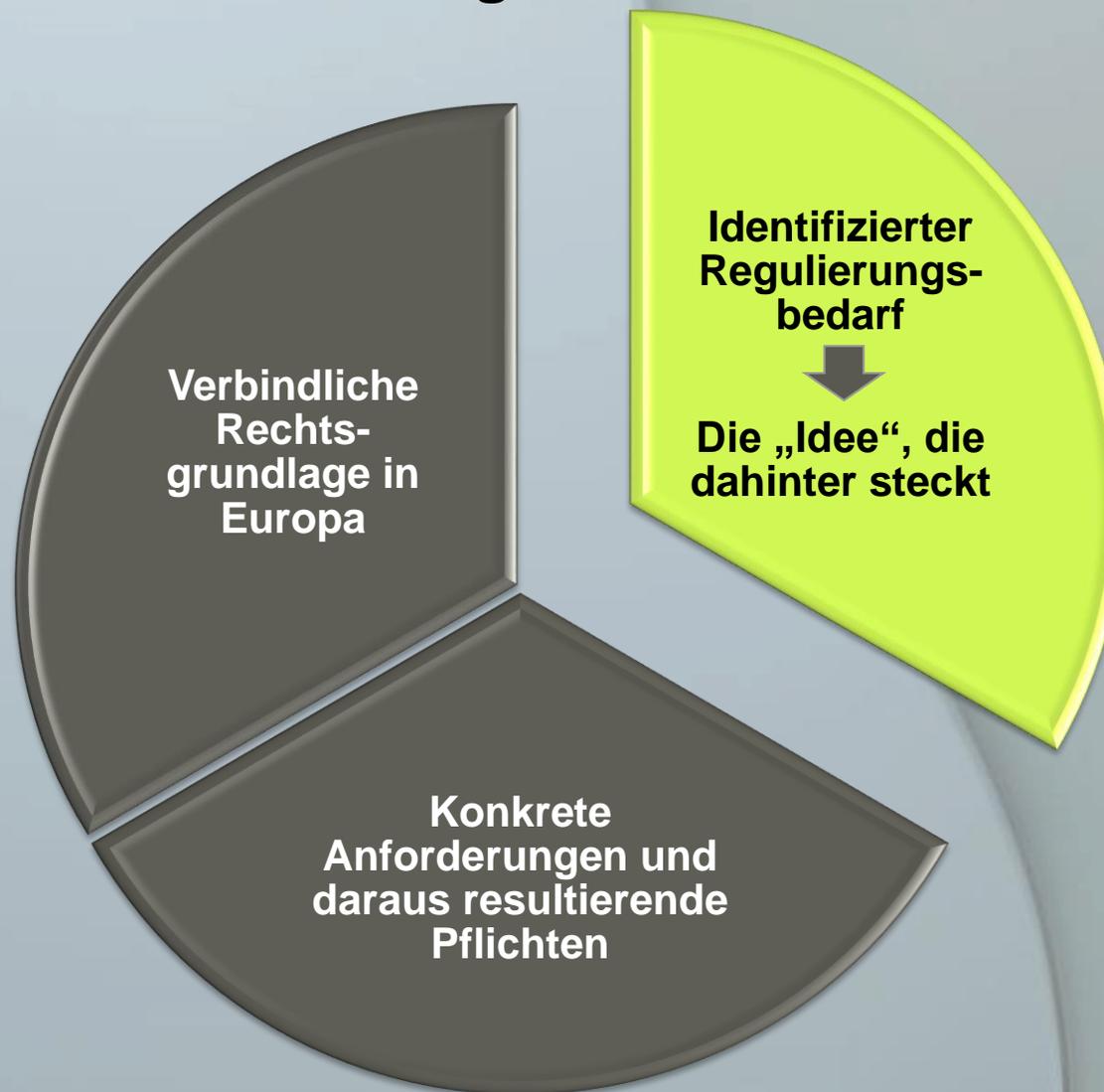
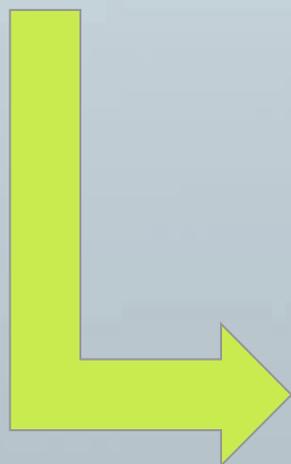
Umsetzung der Anforderungen

- Phasenmodell

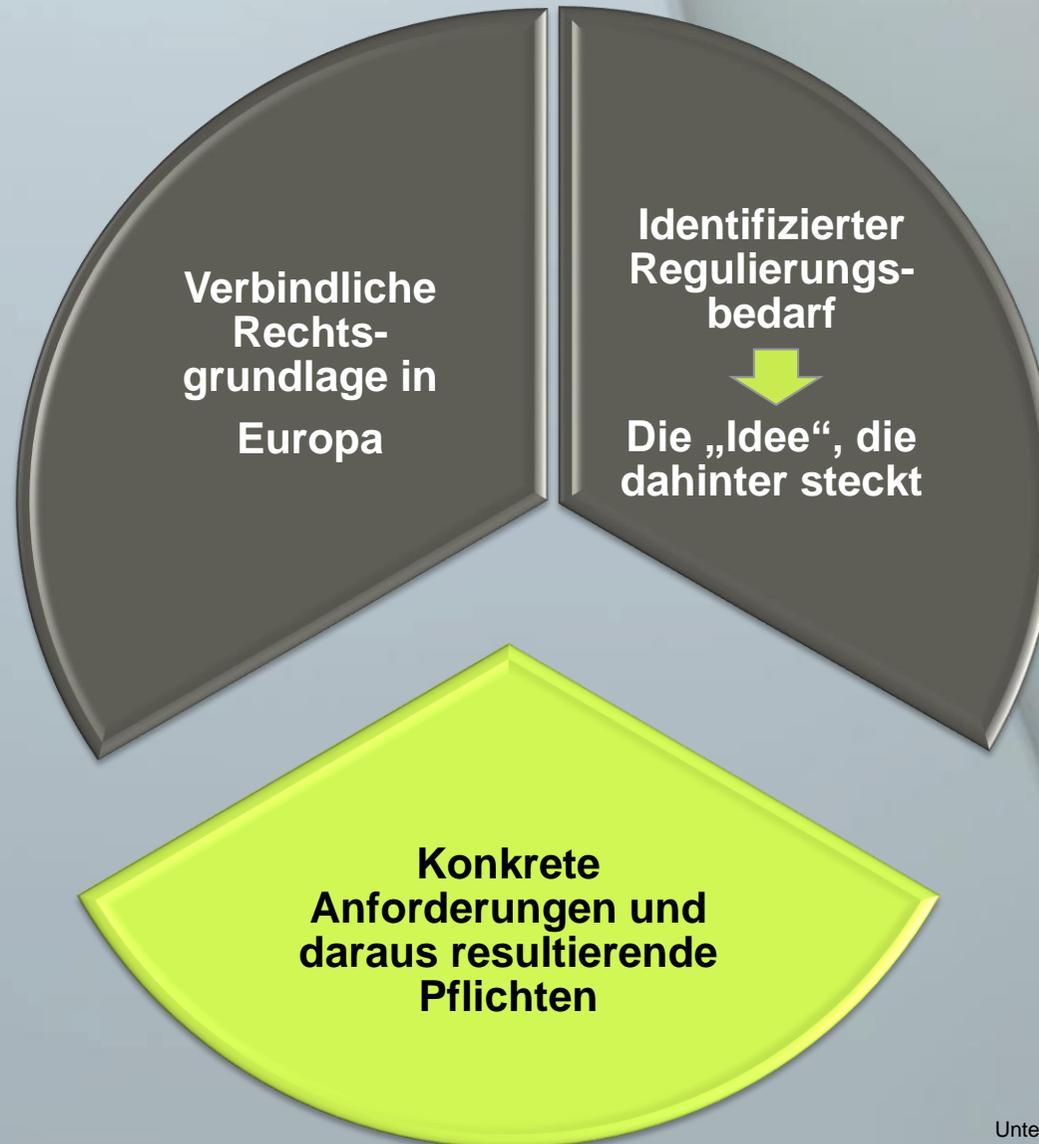
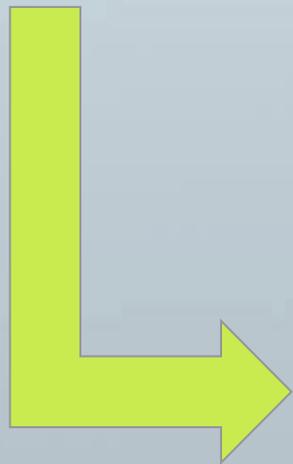
EU Datenschutz - Grundverordnung



EU Datenschutz - Grundverordnung



EU Datenschutz - Grundverordnung



Anforderungen

- Datenschutzgrundsätze
- Rechte der Betroffenen
- Datenschutzkonforme Verarbeitung
- Datenschutzkonforme Technik (Privacy by Design, Privacy by Default)
- Datenschutzkonforme Auftragsverarbeitung
- Verzeichnisverfahren
- Datenschutzkonformes Schutzniveau der Verarbeitung
- Meldung von Schutzverletzungen (Data Breach Notification)
- Datenschutz-Folgenabschätzung (Data Protection Impact Assessment)
- Datenschutzbeauftragter
- Internationaler Datentransfer



Pflichten

- Dokumentationspflichten
- Meldepflichten
- Informations- und Auskunftspflichten
- Rechenschaftspflichten (Accountability)
- Nachweispflicht
- Geeignete technische und organisatorische Maßnahmen (TOM)

Umfangreiche Anforderungen und Pflichten der DSGVO erfordern eine vollumfängliche Strategie, einen strukturierten Ansatz und ein Managementsystem.

Grundsätze bei der Verarbeitung

Grundsätze der Verarbeitung



Rechte...



Rechtmäßigkeit

... auf Berichtigung (Art. 16 DSGVO)

Berichtigung beim Verantwortlichen und bei Datenempfängern

... auf Löschung = „Recht auf Vergessenwerden“ (Art. 17 DSGVO)

Nur, wenn die weitere Verarbeitung nicht erforderlich ist
Löschung beim Verantwortlichen und bei Datenempfängern

... auf Einschränkung (Art. 18 DSGVO)

Nur, wenn die weitere Verarbeitung nicht erforderlich ist
Daten werden gekennzeichnet, um die Weiterverarbeitung zu unterbinden.
Wird angewandt, wenn die Löschung der Daten nur schwer möglich oder die weitere Speicherung erforderlich ist.

... auf Datenübertragbarkeit (Art. 20 DSGVO)

in einem strukturierten, gängigen und maschinenlesbaren Format

... auf nicht ausschließlich automatisierte Entscheidungen (Art. 22 DSGVO)

... den Datenschutzbeauftragten zu konsultieren (Art. 38 Abs. 4 DSGVO)

... auf Widerspruch (Art. 21 DSGVO)

Nur, wenn die Verarbeitung nicht weiter erforderlich ist.

Widerspruch gegen Direktwerbung (Abs. 2)

... auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 Abs. 1 DSGVO)

Grundsätze bei der Verarbeitung

Zweckbindung

Transparenz

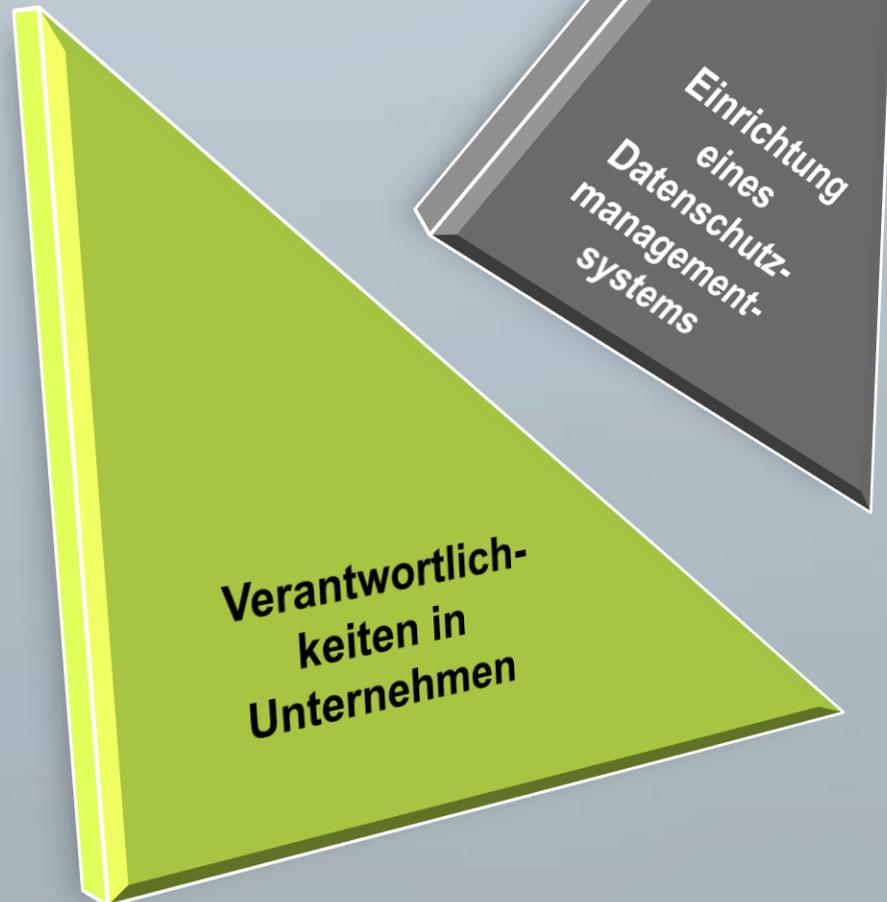
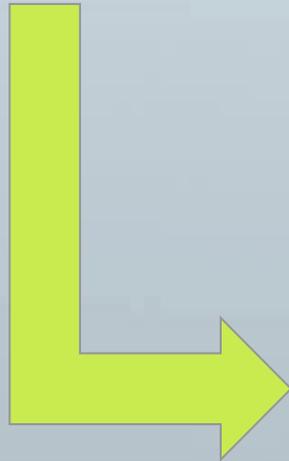
Richtigkeit

Datenminimierung

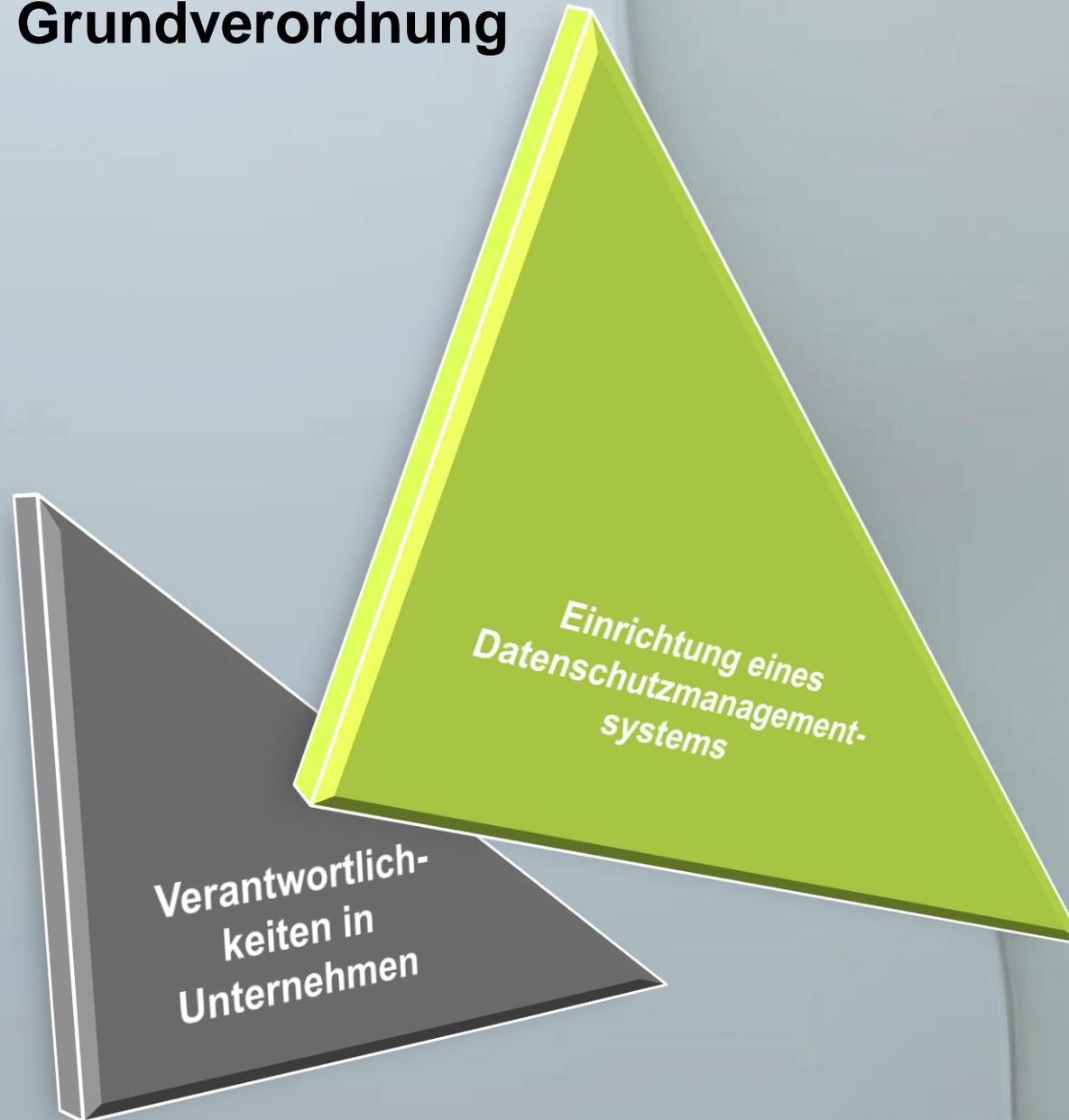
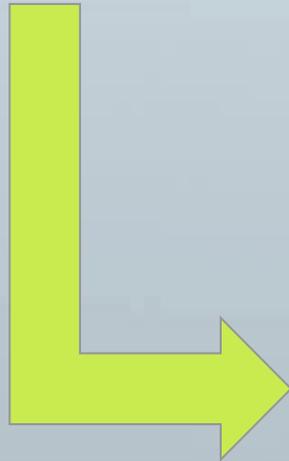
Integrität und
Vertraulichkeit

Rechen-
schaftspflicht des
Verant-
wortlichen

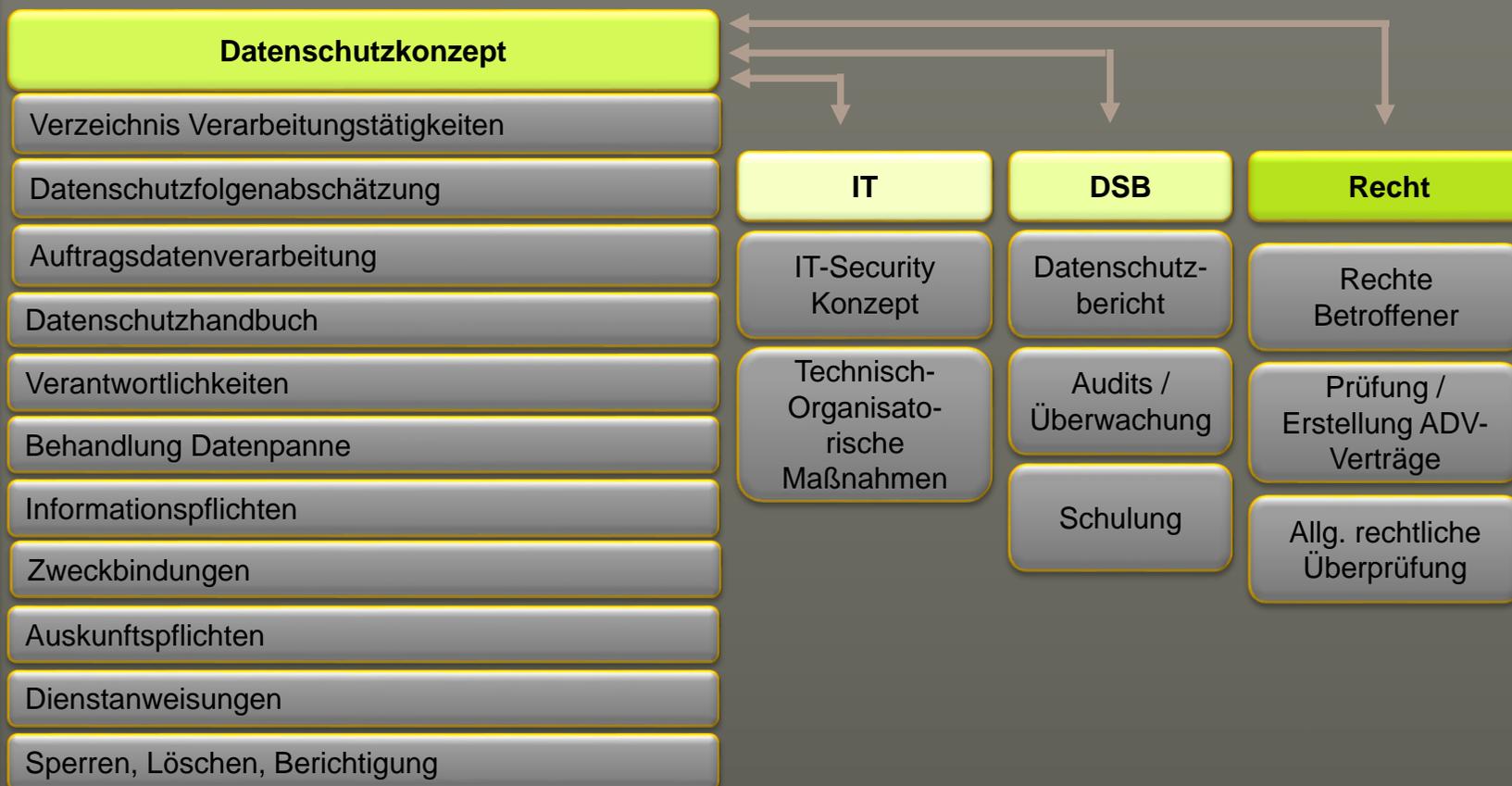
EU Datenschutz - Grundverordnung



EU Datenschutz - Grundverordnung



Datenschutzmanagementsystem



TOM (Technisch Organisatorische Maßnahmen)

Schnittstelle zur IT(-Sicherheit)

Mit geeigneten technischen und organisatorischen Maßnahmen müssen Sie die personenbezogenen Daten, für die Sie verantwortlich sind, schützen und die Verarbeitung gemäß den Prinzipien der DSGVO sicherstellen.

Die DSGVO schreibt folgende Möglichkeiten vor, um mit einem angemessenen Schutzniveau die Sicherheit der personenbezogenen Daten zu gewährleisten (Artikel 32 DSGVO):

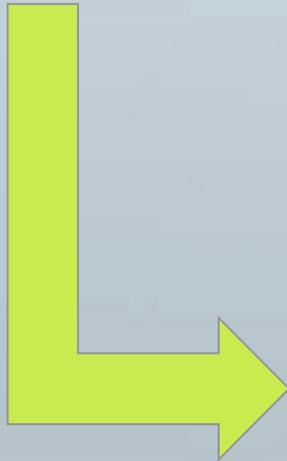
1. Die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;

2. Die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

3. Die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;

4. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

EU DSGVO und Bereederungstätigkeit

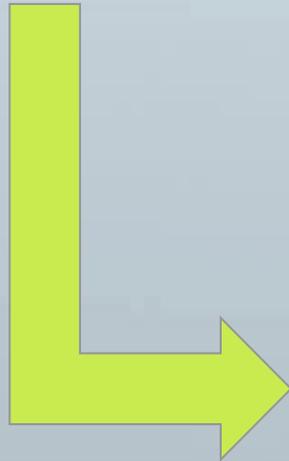


**Personal und Crewing:
Umfangreicher Datenaustausch**

Personal und Crewing



Umsetzung der Anforderung der DSGVO im Unternehmen



Phasenmodell

Meilensteinplan

Meilensteinplan Umsetzung																																			
		1. MS											2. MS											3. MS											
KW		8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34							
Phase 0: Initialisierung		[Green bar from KW 8 to 8]																																	
Durchführung Kickoff		[Grey bar from KW 8 to 8]																																	
Phase I: Istaufnahme und Verarbeitungsverzeichnis		[Green bar from KW 9 to 13]																																	
Aufnahme IST-Verarbeitung		[Grey bar from KW 9 to 9]																																	
Vergleich SOLL -IST nach Datenschutzkriterien		[Grey bar from KW 9 to 12]																																	
Aufbau Verarbeitungsverzeichnis VVT		[Blue bar from KW 9 to 13]																																	
Analyse Schwellwerte SWA		[Grey bar from KW 9 to 12]																																	
Durchführung Datenschutzfolgeabschätzung (DSFA)		[Blue bar from KW 9 to 13]																																	
Aufnahme und Analyse Auftragsverarbeiter AV		[Grey bar from KW 9 to 12]																																	
Phase II: Datenschutzkonzept und DSMS		[Green bar from KW 12 to 26]																																	
Beschreibung organisatorische/technische Maßnahmen (TOM)		[Grey bar from KW 12 to 26]																																	
Erstellung Datenschutzkonzept		[Blue bar from KW 10 to 13]																																	
Dokumentation Datenschutzmanagementsystemen (DSMS)		[Grey bar from KW 10 to 26]																																	
Definition Datenschutzprozesse		[Blue bar from KW 15 to 17]																																	
Phase III: Risikobewertung, Schulung und Audit		[Green bar from KW 24 to 34]																																	
Bewertung Risiko und Abschätzung der Risikofolgen (IT)		[Grey bar from KW 24 to 34]																																	
Schulung Mitarbeiter		[Blue bar from KW 17 to 23]																																	
Audit Datenschutz-Prozesse und Verfahren		[Blue bar from KW 32 to 34]																																	



Herr WP/StB
Andreas Höth
Partner

Baker Tilly

Valentinskamp 88
20355 Hamburg

T: +49 40 600880-368

F: +49 40 600880-452

andreas.hoeth@bakertilly.de



Herr
Martin Beinersdorf
ext. Datenschutzbeauftragter

Outcome Unternehmensberatung GmbH

Hohenstaufenring 47-51
50674 Köln

T: +49 221 2791-0155

martin.beinersdorf@outcome.de



Herr
Bernd Brodersen
Geschäftsführer

Outcome Unternehmensberatung GmbH

Hohenstaufenring 47-51
50674 Köln

T: +49 221 2791-0190

bernd.brodersen@outcome.de