



Mai 2018, Kanzlei WRITZMANN

Rechtliche, organisatorische und technische Aspekte

SOFTCOM

Mit uns können Sie besser kommunizieren



SOFTCOM

Thomas Rathammer / CEO
Rahmon Radaj / Bereichsleiter Technik
Gerhard Burziwal / Bereichsleiter Administration
Christoph Wanjura / Vertrieb DSGVO



WER und WAS ist SOFTCOM?

- **Unabhängiges österreichisches Unternehmen** (Sitz in Wien)
- **Fast drei Jahrzehnte Erfahrung in IT und Telekommunikation**
 - Telekommunikationssektor
 - Öffentlicher Sektor (Verwaltung, Sozialversicherung, Gesundheitswesen, staatliche / teilstaatliche Unternehmen)
 - Transportsektor
 - Banken und Versicherungen
 - Energieversorger
- Aktuell ca. **100** Consultants und IT-Spezialisten
- **ISO-Zertifizierung 9001**
- **Österreichischer Leitbetrieb 2017/18**



SOFTCOM

Mit uns können Sie besser kommunizieren

Referenzkunden

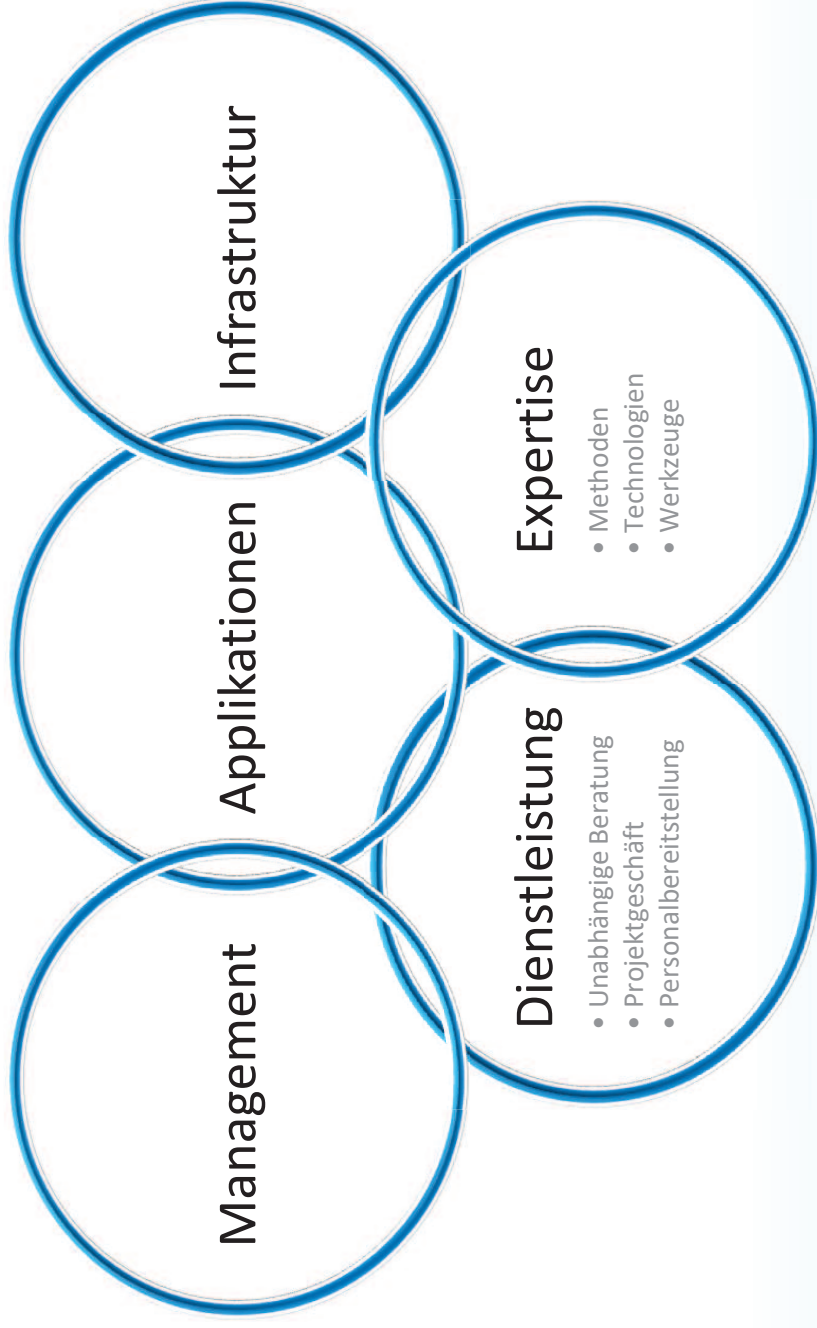


SOFTCOM

Mit uns können Sie besser kommunizieren



SOFTCOM Kompetenzen - Übersicht

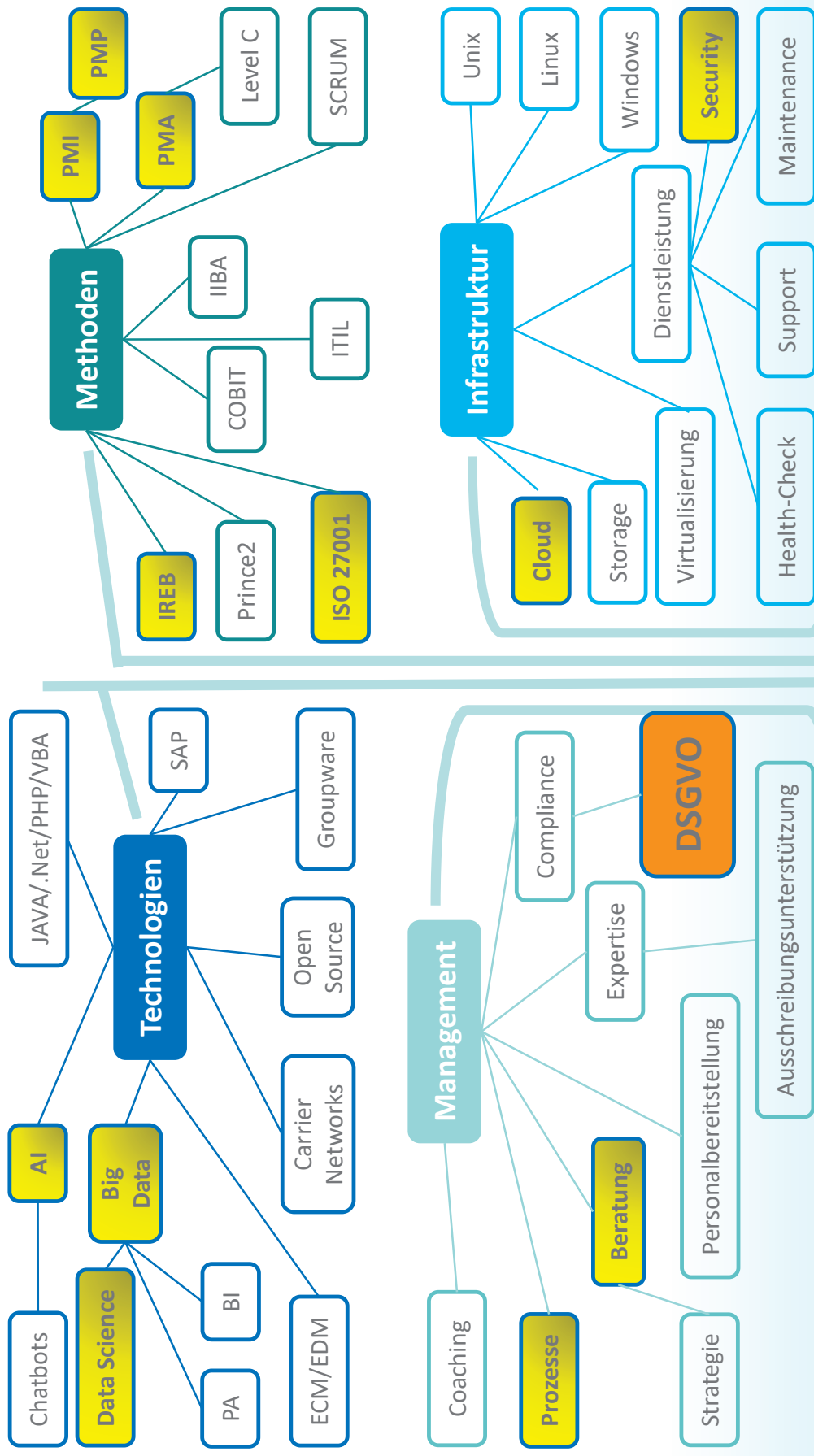


Telekommunikation – Öffentliche Unternehmen – Sozialversicherung
– Banken – Versicherung – Gesundheitswesen

SOFTCOM

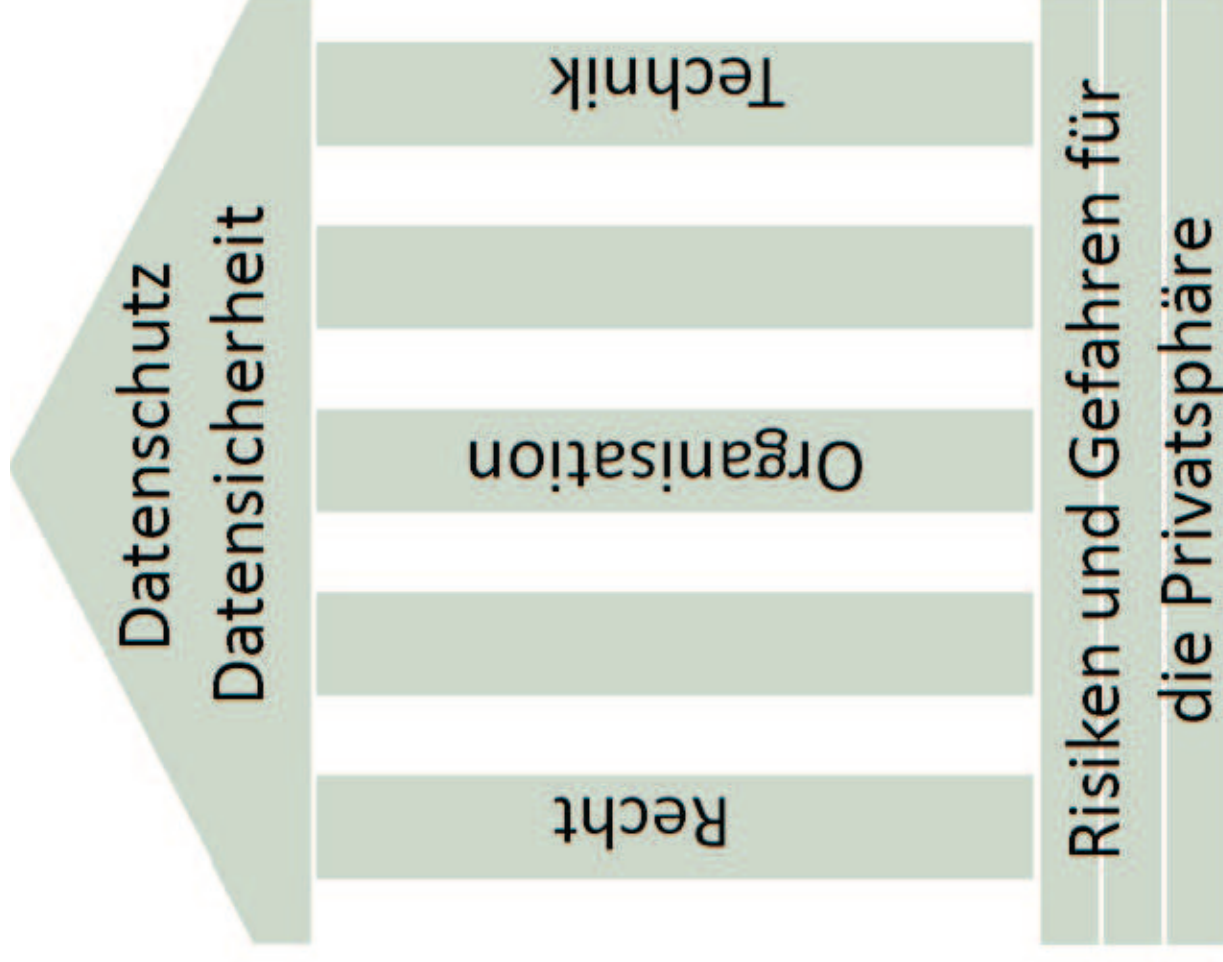
Mit uns können Sie besser kommunizieren

SOFTCOM Kompetenzen - Detail



SOFTCOM

Mit uns können Sie besser kommunizieren



Grundprinzip: mehr Eigenverantwortung, weg von behördlichen Genehmigungen

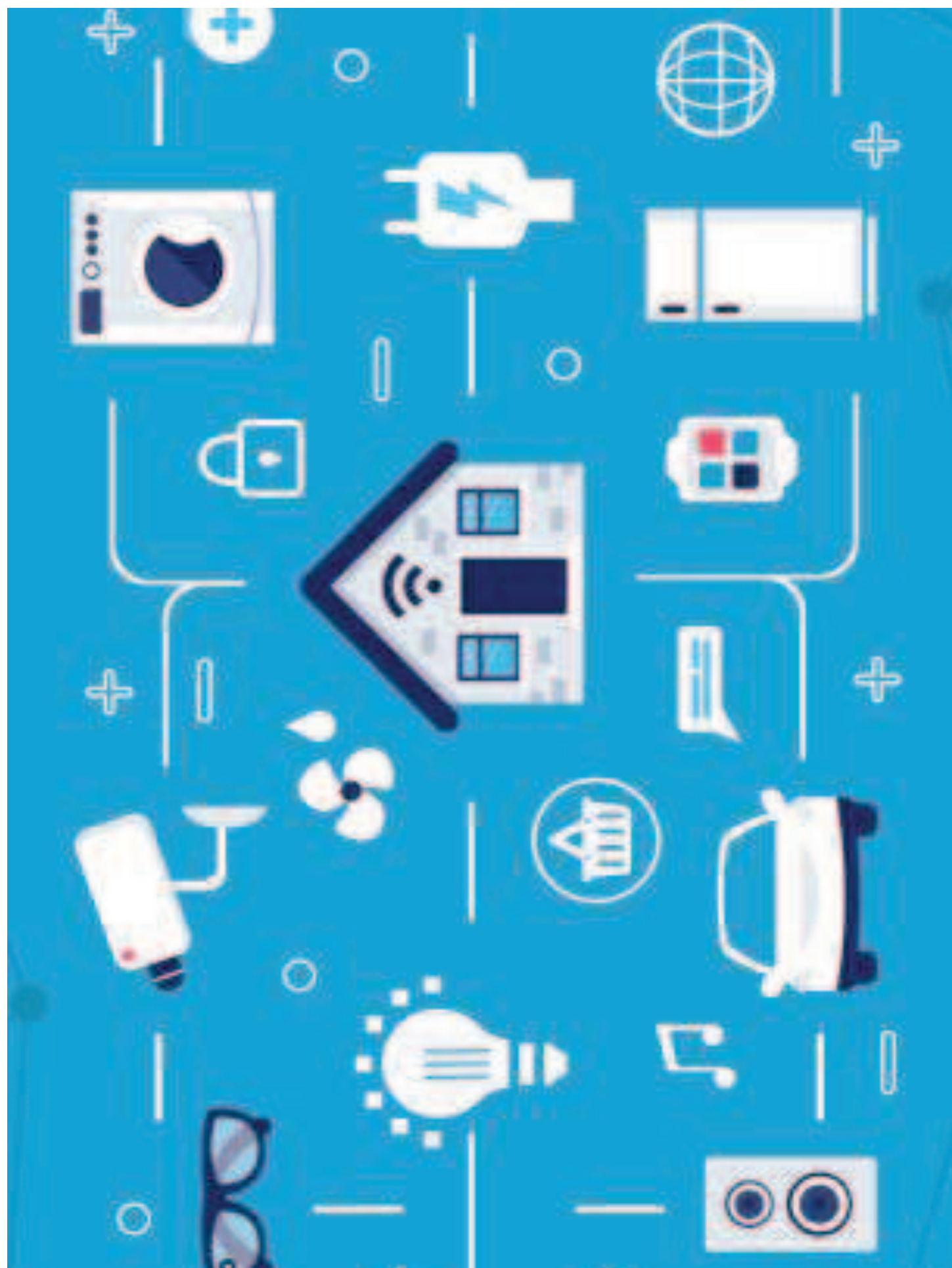
ANGST

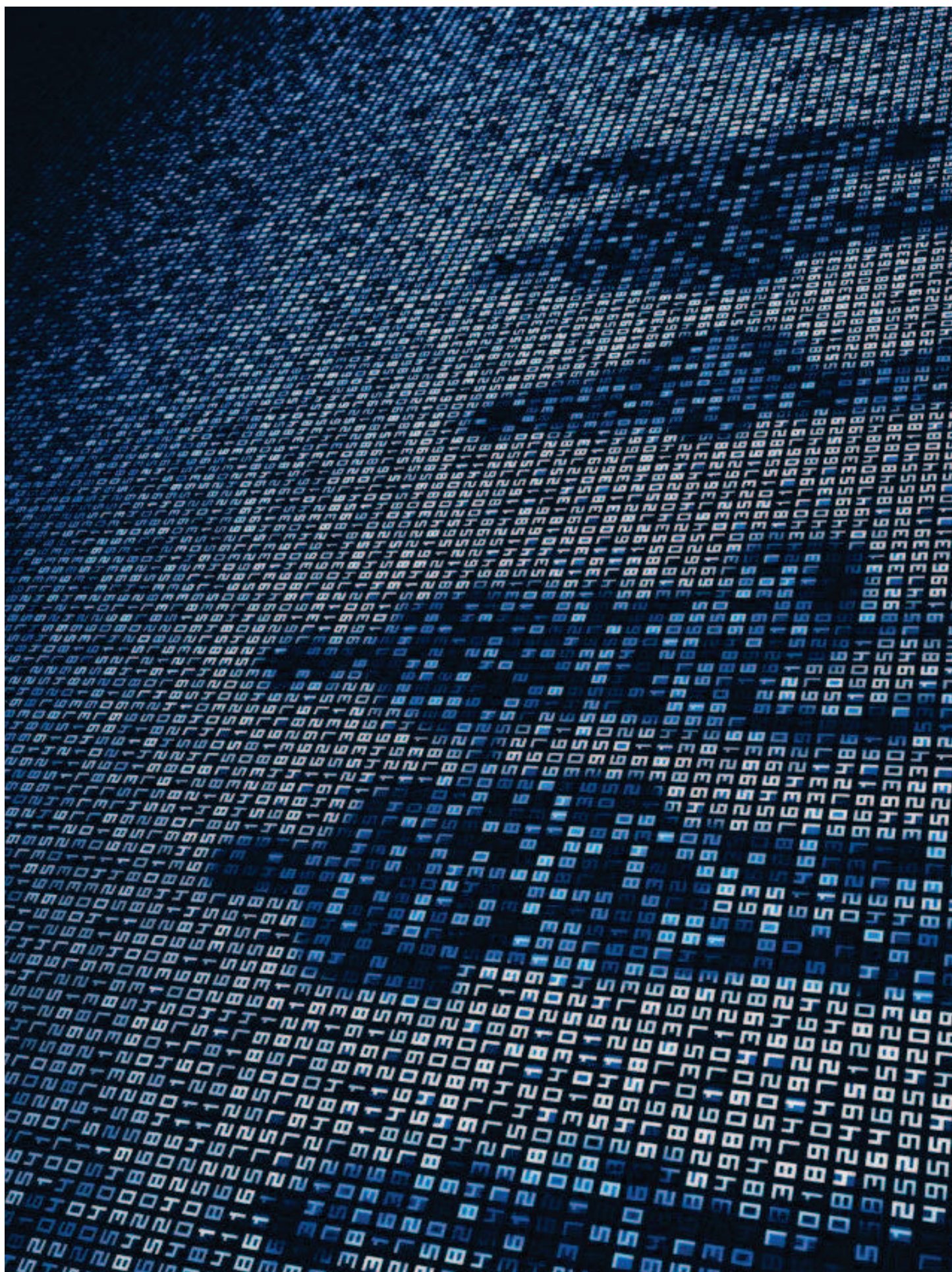
STRAFEN

KOSTEN

BÜROKRATIE

Aberration:









THE CHANCE

DSGVO – Deutsch Deutsch – DSGVO

Mai 2018, Kanzlei WRITZMANN

Rechtliche, organisatorische und technische Aspekte

BURZIWAL/RADAJ (SOFTCOM) – Doppelconference

SOFTCOM

Mit uns können Sie besser kommunizieren

1 Rechtliche Aspekte

- 1.1 Begrifflichkeiten
- 1.2 Neuerungen
- 1.3 Rechtsgrundlagen
- 1.4 Grundsätze
- 1.5 Rechte
- 1.6 Pflichten
- 1.7 DS-Deregulierung

2 Umsetzung

- 2.1 Fact-Finding (Ist-Analyse)
- 2.2 Technik, Risiko & Informationssicherheit
- 2.3 PDCA-Ansatz („fit bleiben“)

3 Dokumentationspflicht

- 3.1 Verarbeitungsverzeichnis
- 3.2 Stammdaten

4 Ende/Fragen



*Stellen Sie sich vor es ist
DSGVO ...*

und keiner geht hin!

1.1 Begrifflichkeiten

- **DatenSchutzGrundVerOrdnung**
(GeneralDataProtectionRegulation)
- Personenbezogene Daten (der „Betroffenen“)
- Sensible Daten
- Datenverarbeitung
- Technologieneutral
- Profiling/Scoring
- Einwilligung & Kopplungsverbot (Opt-In)

1.2 Neuerungen

- Stärkere Nutzer- bzw. Betroffenenrechte
- Höhere Verantwortung (Verantwortlicher\Auftragsverarbeiter)
- Höhere Strafen bzw. Bußgelder
- Verzeichnis von Verarbeitungstätigkeiten (statt DVR)
- Markortprinzip
- Datenschutz durch Technikgestaltung



Die Verarbeitung von
personenbezogenen Daten
ist ...

VERBOTEN!

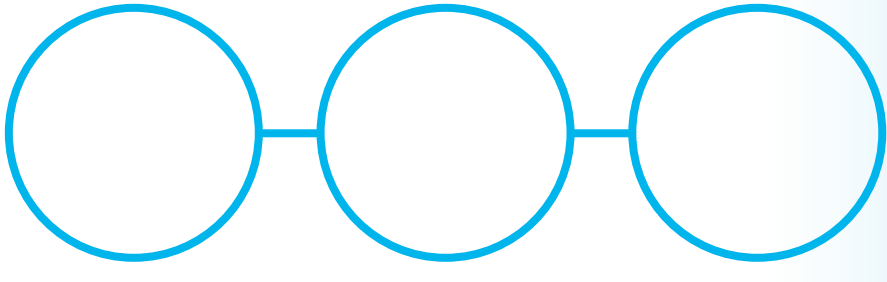
1.3 Rechtsgrundlagen

Verbot mit Erlaubnisvorbehalt, wenn ...

- ... der Betroffene zustimmt
- ... die Verarbeitung für die Vertragserfüllung notwendig ist
- ... eine gesetzliche Verpflichtung es notwendig macht
- ... der Schutz lebensnotwendiger Interessen Vorrang hat
- ... die Verarbeitung im öffentlichen Interesse liegt
- ... die Verarbeitung für legitime Zwecke des Verantwortlichen oder eines Dritten notwendig ist (Achtung: **Interessensabwägung!**)

1.4 Grundsätze der Verarbeitung (Art.6)

- Zweckbindung
- Rechtmäßigkeit und Transparenz
- Datenminimierung (Need2Know)
- Richtigkeit
- Speicherbegrenzung



1.5 Rechte

... der Betroffenen auf:

- Auskunftsrecht
- Berichtigung
- Widerspruchsrecht
- Einschränkung der Verarbeitung
- Löschung („Vergessenwerden“)
- Datenübertragbarkeit
- Beschwerderecht / Schadenersatz

1.6 Pflichten

... der Verantwortlichen:

- Datenschutzbeauftragter(?)
- Technisch-organisatorische Maßnahmen
- Dokumentations- bzw.

Rechenschaftspflicht

- Verarbeitungsverzeichnis
- Data-Breach (Logbuch)

... der Auftragsverarbeiter:

- Verarbeitungssverzeichnis
- Kooperation mit DSB
- Risikoanalysen & Unterstützung
- Warnpflicht / Subunternehmer

1.7 DS-Deregulierungsgesetz

... vom 20.4.2018

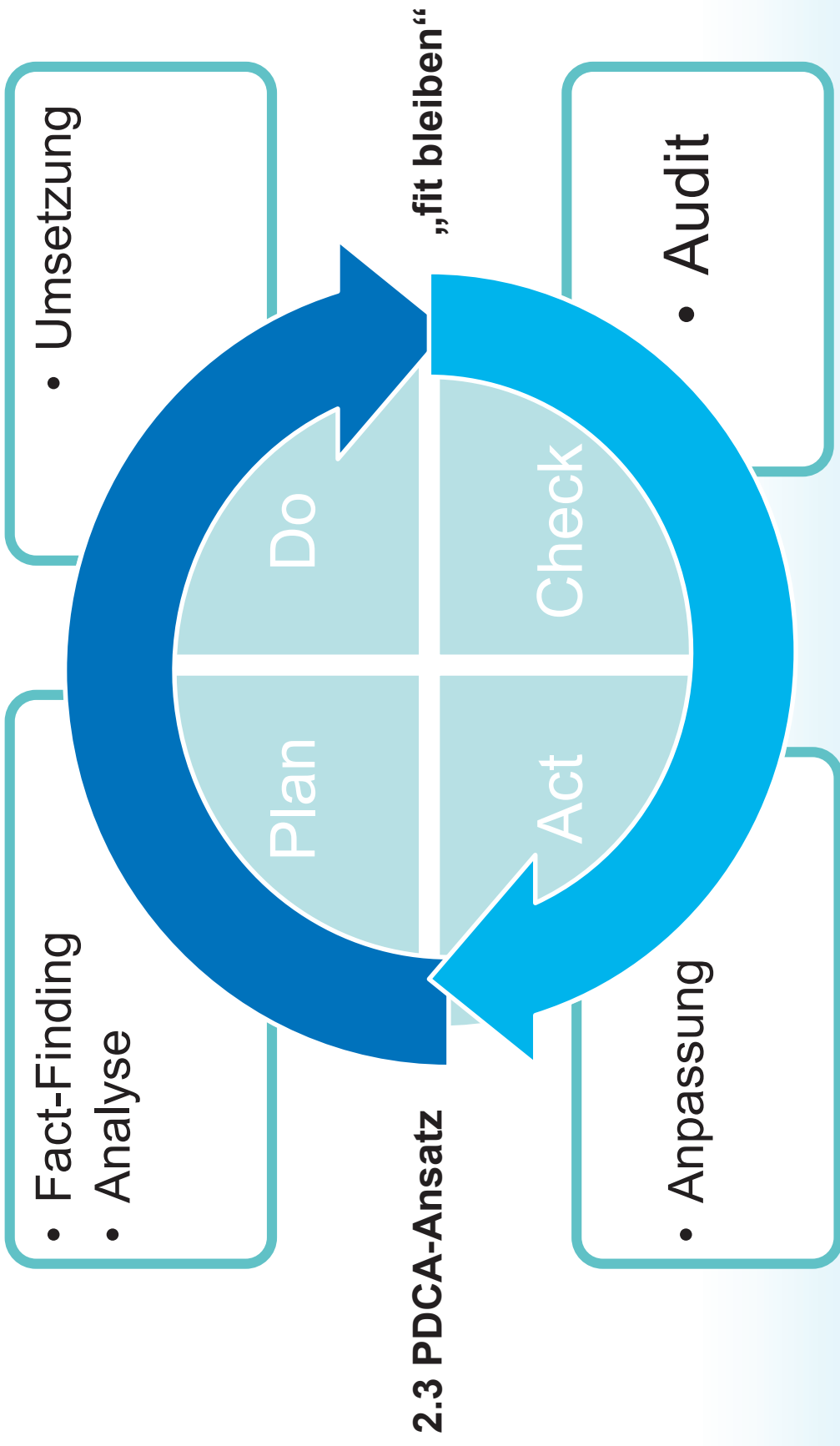
- Verwarnen statt Strafen (bei Erstvergehen)
- Aufweichung der Auskunftspflicht („Betriebsgeheimnis“)
- Behörden vollkommen straffrei
- Management-Haftung deutlich reduziert
- Freibrief für Künstler (aber auch andere)
- Keine Sammelklagen möglich

2.1 Fact-Finding (Ist-Analyse)

- Bestehende DVR-Meldung
- Bestehende Frameworks nutzen (DSMS, ISO etc.)
- Interne Abläufe durchleuchten (Prozesse)
- Tools/Software/Apps/Checklisten
- Über die Grenzen schauen (nur Impulse)
- Externe Hilfe: Fachkundige Anleitung/Beratung

2.2 Technik, Risiko & Informationssicherheit

- Privacy by Design / Privacy by Default
- Pseudonymisierung / Anonymisierung
- Verschlüsselung
- Risikobasierter Ansatz
- Datenschutzfolgeabschätzung (DSFA)
- Vertraulichkeit/Verfügbarkeit/Integrität



3.1 Verarbeitungsverzeichnis (nach Art. 30)

- Kontaktdaten
- Zweck
- Rechtsgrundlage
- Datenkategorien
- Löschfristen
- Empfänger

Verarbeitungsverzeichnis SOFTCOM (DSGVO)

Nr.	Prozess	Datenfluss (Schnittstellen)	Zweck	Rechtsgrundlage	Betroffener
1	Recruiting	Mail (extern) > Exchange > MS-Access > (Personalfragebogen) > BewerberDB	Bereitstellung von Ressourcen	Vertragserfüllung und Einwilligung	Bewerber
	Personal	PersonalDB > Excel > BMD (Import) > Mail	Anmeldung bei Krankenversicherung und Abrechnung von Lohnbezügen.	Gesetzliche Anforderungen und Erfüllung des (Dienst-)Vertrages.	Mitarbeiter
	Personalentwicklung	PersonalDB > Excel > BMD (Import) > Mail	Überwachung/Steuerung der Mitarbeiterentwicklung	Gesetzliche Verpflichtung zur Zeitaufzeichnung der Mitarbeiter und wirtschaftliches Interesse.	Mitarbeiter
Führungsprozesse					
Kernprozesse					
4	Projektdurchführung	Formular (Mail)	Mitarbeiterentwicklung bzw. -entlohnung.	Berechtigtes wirtschaftliches Interesse.	Mitarbeiter
Unterstützende Prozesse					
7	allgemein	Mitarbeiter > Kunden/Kollegen/Vorgesetzter/GF > Admin	Dokumentation von Anwesenheiten, Verrechnung von Diäten bzw. Spesen.	Gesetzliche Verpflichtung (Zeitaufzeichnung), Vertragserfüllung (Kunde) und eigenes wirtschaftliches Interesse.	Mitarbeiter

Dokumentationspflicht

Dokumentationspflicht

Stammdaten und Kontaktliste der SOFTCOM Consulting GmbH (12., Bischoffgasse 13)			
Funktion	Name	Telefon	Data-Breach (Verständigung) Datenschutz (Auskunft)
Geschäftsleitung (gesetzliche Vertretung)			x
Prokurist/Datenschutzkoordinator (intern)			x
Datenschutzexperte			x
DSGVO Vertrieb			
DSGVO Administration			x
DSGVO Projektunterstützung			x
Corporate Identity und Website			x



SOFTCOM & DSGVO

Wie kann SOFTCOM Ihnen helfen?



Mit uns können Sie besser kommunizieren



SOFTCOM & DSGVO

- **Wir machen Ihr Unternehmen DSGVO-FIT!**
- **Der One-Stop-Shop SOFTCOM:**
 - alle notwendigen Kompetenzen aus einer Hand
 - Zertifiziertes DSGVO-Know-how, Projektmanagement
Expertise, Prozessmanagement Expertise, Technische
Expertise, Rechtliche Expertise



SOFTCOM & DSGVO: Unsere Leistungen

Awareness

- Management-Awareness sicherstellen
- Sensibilisierung bzw. Schulung der Mitarbeiter

Analyse

- Risiko-Analyse
- GAP-Analyse zur Identifizierung der strategischen Ziele und operativen Handlungsfelder (Infrastruktur, Security etc.)
- Management Summary
- Optional: Daten- und Prozesslandkarte

**Umsetzungs-
begleitung**

- Entwicklung der Datenschutzrichtlinien und Implementierung von IT-Security Vorgaben (Firewall, Berechtigungen, Verschlüsselung etc.)
- Analyse der meldepflichtigen Datenanwendungen
- Verfahrensverzeichnis /Dokumentation
- Risikofolgeabschätzung und TOMs

Review

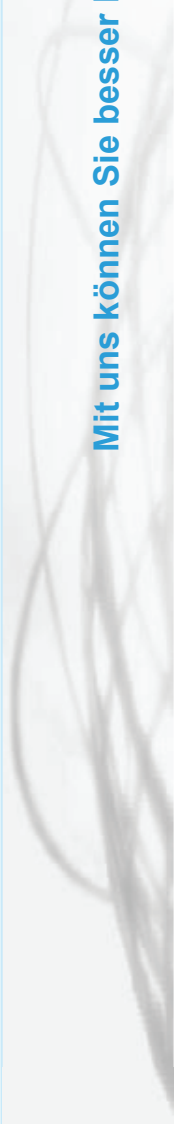
- Regelmäßige Audits
- Maßnahmenbericht und kontinuierliche Verbesserung
- Unterstützung bei Kommunikation mit Datenschutzbehörde



Danke für die Aufmerksamkeit!



Mit uns können Sie besser kommunizieren

A series of thin, grey, overlapping curved lines that create a sense of motion and flow, positioned behind the text in the bottom right corner.