PSW GROUP

EU-DATENSCHUTZ-GRUNDVERORDNUNG EU-DSGVO

Was kommt?
Was bleibt?

§ DS-GVO

Die neue EU-Verordnung ist in Kraft getreten

DIE DS-GVO IST AB 25. MAI 2018
VERBINDLICH FÜR ALLE
UNTERNEHMEN IN EUROPA!

BALD SCHMERZEN SANKTIONEN RICHTIG!

Gemäß Art. 83 Abs. 4 DS-GVO:

Bis zu **10.000.000,00 Euro** oder
bei Unternehmen bis zu
2 % des weltweit erzielten Jahresumsatzes!
(Nach Maximalprinzip!)

GELDBUßEN

ES GEHT NOCH TEURER!

Gemäß Art. 83 Abs. 5 DS-GVO:

Bis zu **20.000.000,00 Euro** oder
bei Unternehmen bis zu
4 % des weltweit erzielten Jahresumsatzes!
(Nach Maximalprinzip!)

GELDBUßEN

GRUND ZUR FREUDE:

WERBUNG DARF SEIN - ZUWEILEN

“ONE CONTINENT, ONE LAW„

Vollharmonisierung des Datenschutzrechts der EU

GLEICH **HOHE DATENSCHUTZSTANDARDS FÜR ALLE BETROFFENEN** UND **RECHTSSICHERHEIT FÜR UNTERNEHMEN**

AUFTRAGSDATEN-VERARBEITUNG (ADV)

Zwar orientieren sich die neuen Regelungen inhaltlich an § 11 BDSG, jedoch existieren einige relevante Unterschiede!

ERHEBEN, VERARBEITEN ODER NUTZEN VON PERSONENBEZOGENEN DATEN

DURCH AUFTRAGNEHMER

GRUNDSÄTZLICHE ÄNDERUNGEN & ANFORDERUNGEN

Sprachliche Änderung: "Auftragsverarbeiter" und "für die Verarbeitung Verantwortlicher" sind neue Begriffe

DER AUFTRAGSVERARBEITER MUSS **SORGFÄLTIG** UND **UNTER BERÜCKSICHTIGUNG TECHNISCHER SOWIE ORGANISATORISCHER MASSNAHMEN (TOM)** AUSGEWÄHLT WERDEN

(Regelung analog zu § 11 BDSG)

MITVERANT-WORTUNG DES AUFTRAGS-VERARBEITERS

Art. 28 Abs. 10 DS-GVO

BEI **VERSTOß** WIRD DER
AUFTRAGSVERARBEITER SELBST
ZUM **VERANTWORTLICHEN!**

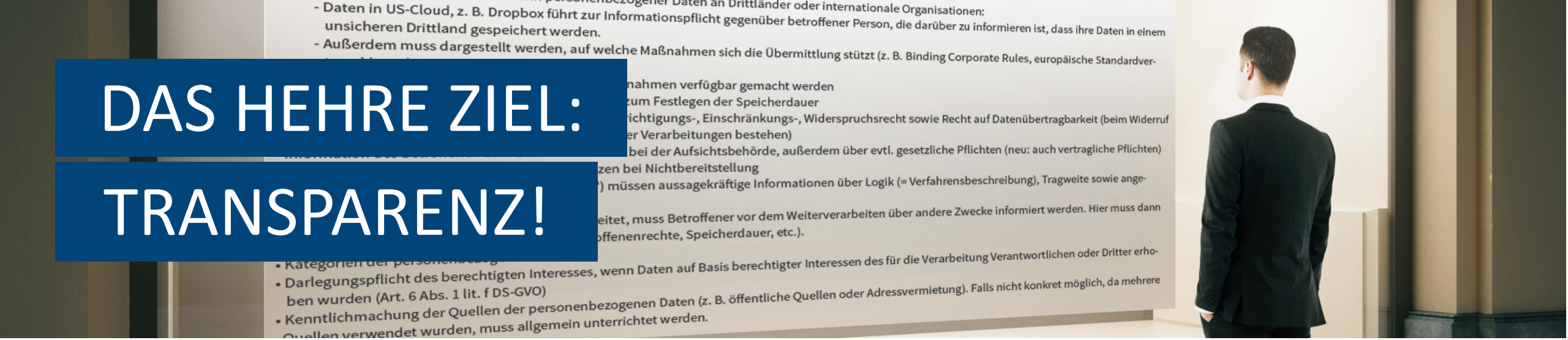
WAS TUN?

Nutzen Sie die Übergangsphase bis 2018

NEUVERTRÄGE BERÜCKSICHTIGEN IDEALERWEISE BEREITS DIE KÜNFTIGE RECHTSLAGE, ALTVERTRÄGE PRÜFEN UND ANPASSEN!

WAS SOLLTE ZUKÜNFTIG IN IHRER ADV STEHEN:

- Aufgabenverteilung gemäß DS-GVO-Pflichten
- Wie wahren Sie die Betroffenenrechte?
- Wer erfüllt die Informationspflichten nach Art. 13 f. DS-GVO?
- Festlegen von Kontaktstellen (Verantwortlicher Verarbeiter, ggf. Stellvertreter und DSB) für den Betroffenen
- Beschreibung von Funktion & Beziehung zum Betroffenen inkl. Mitteilung dieser Beschreibungen an den Betroffenen.



DAS HEHRE ZIEL: TRANSPARENZ!

INFORMATIONSPFLICHTEN

Art. 13 & 14 DS-GVO beschreiben die neuen Informationspflichten, die deutlich über die bisherigen Pflichten des BDSG hinausgehen

ZU SCHAFFENDE **TRANSPARENZ** SOLL ES DEM EINZELNEN ERMÖGLICHEN, ZU ERKENNEN, **WER WAS WANN WOZU** ÜBER IHN ERHEBT, VERARBEITET UND/ODER SPEICHERT

INFOPFLICHT BEI DIREKTERHEBUNGEN

Art. 13 DS-GVO

- Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DS-GVO)
- Übermitteln personenbezogener Daten an Drittländer oder internationale Organisationen (z.B. Clouddienste, Dropbox, etc.)

NOCH MEHR PFLICHTEN

Zum Gewährleisten der fairen & transparenten Datenverarbeitung sind weitere Informationen vorgeschrieben:

- Speicherdauer
- Betroffenenrechte
- Beschwerderecht bei der Aufsichtsbehörde
- Auskunft zu "Profiling“
- Zweckbestimmung

PRINZIPIEN DER DATENVERARBEITUNG

Art. 5 DS-GVO

WORAUF MÜSSEN SIE ACHTEN?

- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität & Vertraulichkeit
- Rechenschaftspflicht (Accountability)

ZERTIFIZIERUNG HILFT!

Ob ISIS12 für KMU oder ISO 27001 für mittlere bis große Unternehmen:

Da zur Zertifizierung das Einhalten der Prinzipien zur Datenverarbeitung gemäß § 5 DS-GVO notwendig ist, sind Sie zertifiziert definitiv auf der sicheren Seite!

Zertifizierungen belegen, dass Sie sich an die Grundsätze zur Datenverarbeitung halten.

Die DS-GVO besagt:

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

BDSG ‡ DS-GVO

SCHUTZWÜRDIGES INTERESSE ‡ INTERESSEN BZW. GRUNDRECHTE UND GRUNDFREIHEITEN

ZWECKBINDUNGS-GRUNDSATZ

Der Teufel steckt im Detail

- Konkreter Verarbeitungszweck
- Bestimmte Zweckbindung
- Interessenabwägung

RECHTSKONFORME EINWILLIGUNGEN

Basis:
"Grundrecht auf informationelle Selbstbestimmung" (= Grundrecht auf Datenschutz) gemäß Art. 2 Abs. 1, Art. 1 Abs. 1 GG

DS-GVO GESTALTET GRUNDRECHT EUROPAWEIT AUS

- Zur wirksamen Einwilligung bedarf es eines Opt-Ins

ANFORDERUNGEN AN EINE WIRKSAME EINWILLIGUNG

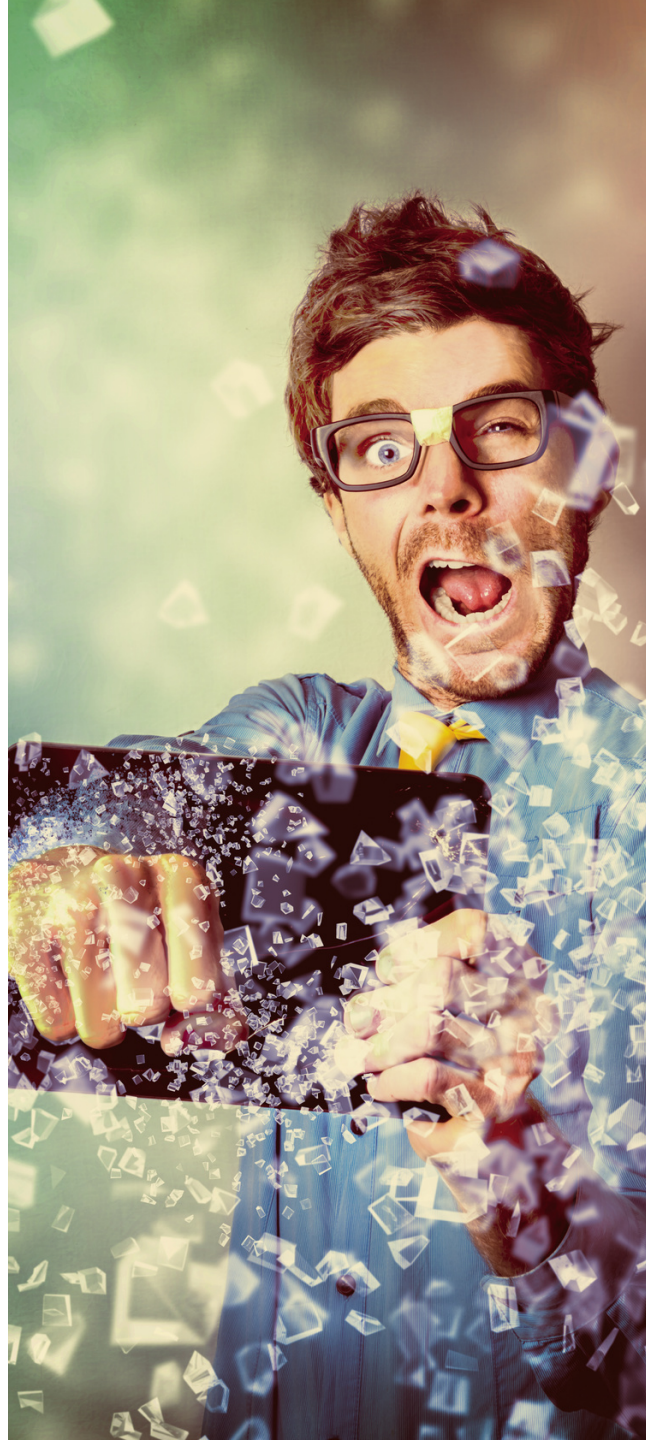
gemäß Art. 7 DS-GVO

- Eine Einwilligung, die mit anderen Erklärungen schriftlich erteilt wird, ist besonders hervorzuheben
- Echte Wahl für Betroffene ohne Nachteile

AUSKUNFTSRECHT BETROFFENER PERSONEN

gemäß Art. 15 DS-GVO

- Jeweilige Daten und Verarbeitungszwecke
- Kategorien der personenbezogenen Daten
- Empfänger, an die Daten weitergegeben werden oder weitergegeben wurden
- Geplante Speicherdauer
- Daten-Herkunft (wenn nicht beim Betroffenen selbst erhoben)
- Vorliegen von automatisierten Entscheidungsfindungen inkl. etwaigem Profiling
- Berichtigung und/oder Löschung personenbezogener Daten
- Beschwerderecht bei Aufsichtsbehörden



RECHT AUF LÖSCHUNG
("RECHT AUF VERGESSENWERDEN")

gemäß Art. 20 DS-GVO

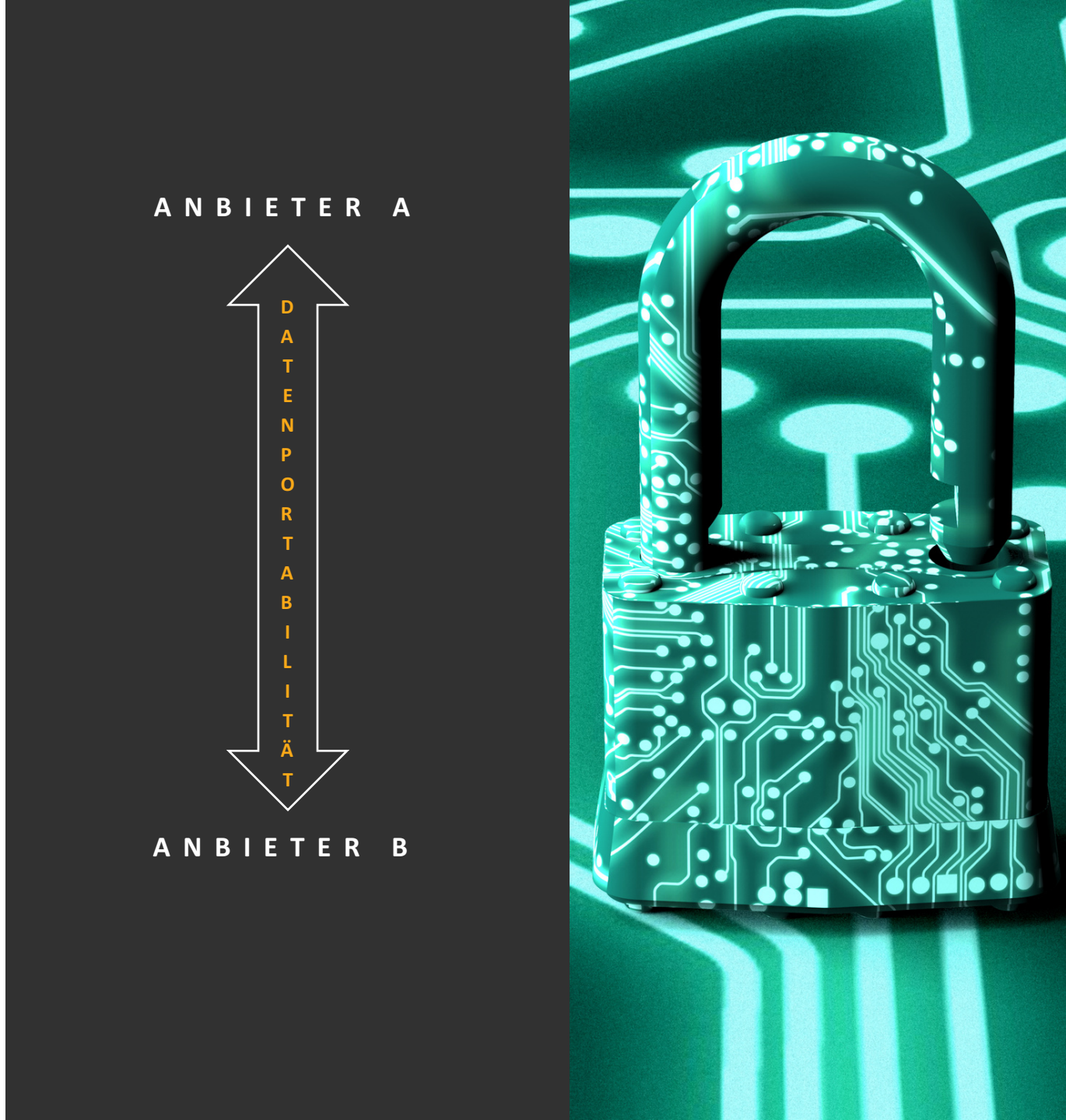
- Bestehen gesetzliche Aufbewahrungsfristen, scheidet ein Löschen gemäß Art. 17 Abs. 3b DS-GVO weiterhin aus

- Der für die Verarbeitung Verantwortliche muss sämtliche Verantwortlichen ermitteln und über Löschung informieren

RECHT AUF DATENÜBERTRAGBARKEIT

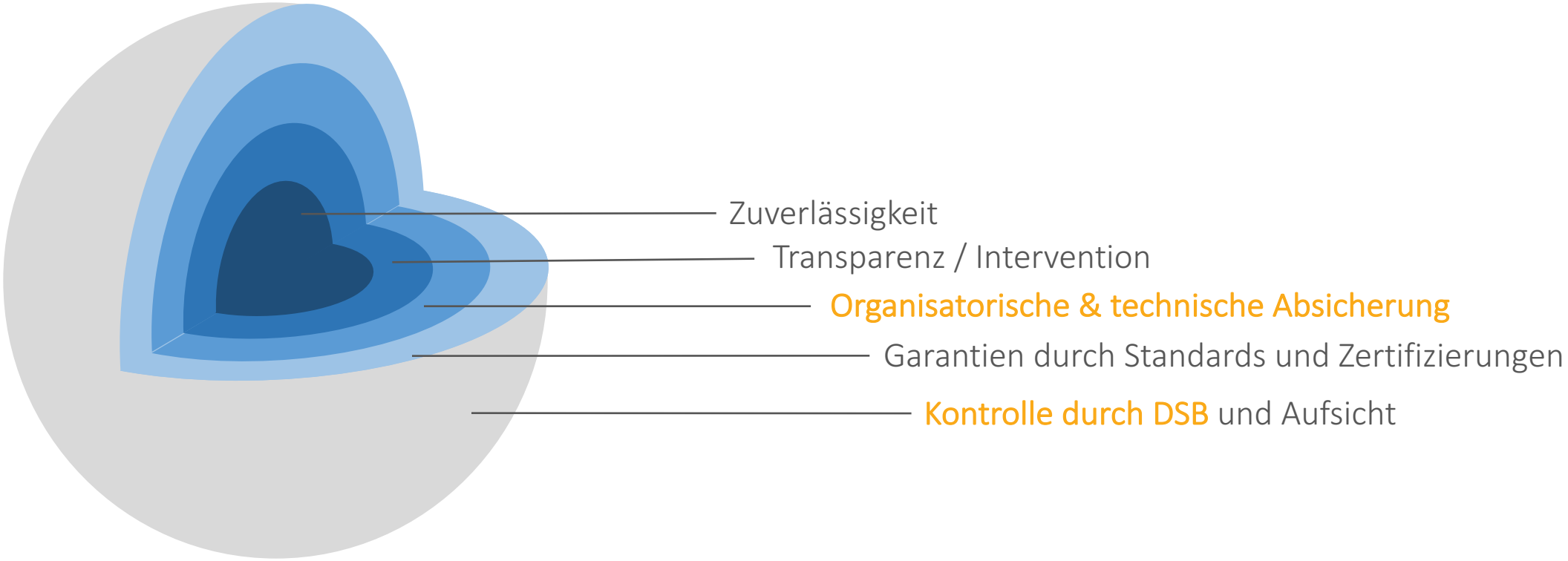
gemäß Art. 20 DS-GVO

AUF WUNSCH EINES KUNDEN PERSONENBEZOGENE DATEN SICHER, ABER **KOMPATIBEL** ZU GÄNGIGEN SYSTEMEN TRANSFERIEREN.



AUFBAU DER DS-GVO

Die neue Rolle des Datenschutzbeauftragten (DSB) und das sich daraus ableitende Schutzkonzept



DSB:PFLICHT ODER KÜR?

Verpflichtend für ...

- ... öffentliche Stellen
- ... alle Unternehmen, die Daten verarbeiten

BESTELLUNG DES DSB

Achten Sie auf die notwendige Qualifikation!

- Unternehmen können sich einen DSB "teilen"
- Interner oder externe DSB

AUFGABEN-STELLUNG DES DSB

gemäß Art. 39 DS-GVO

DER DSB **UNTERRICHTET UND BERÄT** ZU DATENSCHUTZPFLICHTEN, **KONTROLLIERT PROZESSE** UND **STEHT DER AUFSICHTSBEHÖRDE** BEI RÜCKFRAGEN **ZUR VERFÜGUNG .**

DATENSCHUTZ-FOLGENABSCHÄTZUNG

gemäß Art. 35 DS-GVO

Der für die Verarbeitung Verantwortliche muss eine Datenschutzfolgenabschätzung durchführen, wenn …

- … die Verarbeitungsform mit hohen Risiken für die persönlichen Rechte & Freiheiten verbunden ist und insbesondere, wenn …
- … dafür neue Technologien verwendet werden

KONSULTATIONSPFLICHT

gemäß Art. 36 DS-GVO

- Der für die Verarbeitung Verantwortliche haben bei hohen Risiko Konsultationspflicht gegenüber Aufsichtsbehörden
- Vor der Datenverarbeitung
- Aufsichtsbehörde gibt Empfehlungen ab

DATENSCHUTZ RECHTSSICHER ORGANISIEREN

Ein Datenschutzmanagementsystem hilft Ihnen

- Risikobasiert
- Privacy by Design
- Dokumentationspflichten
- Rechenschaftspflichten

Zertifizierungen weisen eine rechtssichere Datenschutzorganisation nach!

PDCA-MODELL

Zur Datenschutzorganisation

PLAN:

Risikobewertung unter Einbeziehung von:
Verarbeitungsart, Verarbeitungsumfang,
Verarbeitungsumstand & Verarbeitungszweck
Eintrittswahrscheinlichkeit
Risiken für persönliche Rechte & Freiheiten

DO:

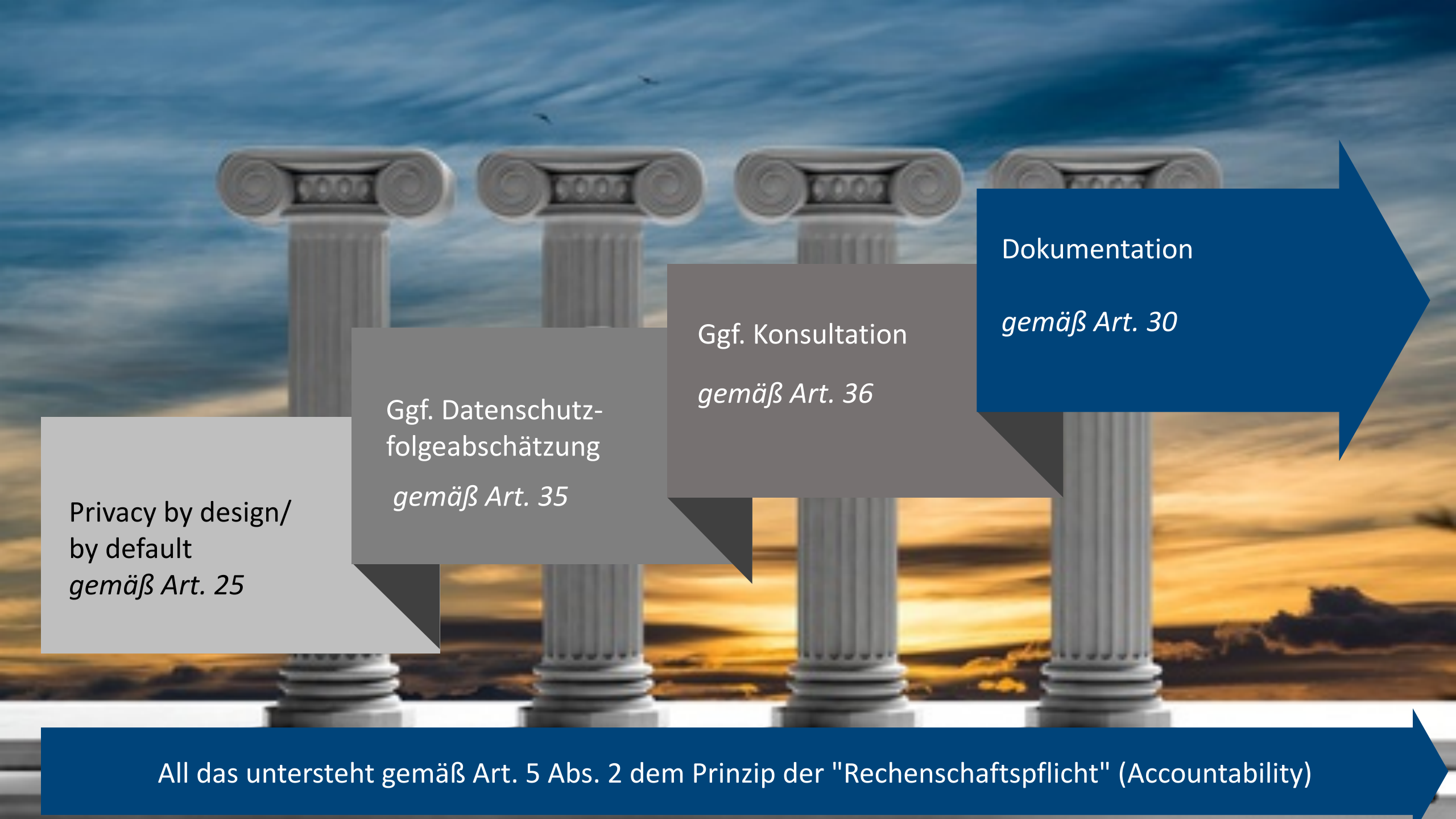
Geeignete Technik & Organisation
Datenschutzvorkehrungen gemäß
Datenschutzmanagementsystem
Rechtssichere Datenverarbeitung
nachweisen

CHECK:

Maßnahmen überprüfen

ACT:

Etwaiges Aktualisieren/ Anpassen
bisheriger Maßnahmen
Optimieren des Ist-Zustands


Privacy by design/
by default
gemäß Art. 25
Ggf. Datenschutz-
folgeabschätzung
gemäß Art. 35
Ggf. Konsultation
gemäß Art. 36
Dokumentation
gemäß Art. 30
All das untersteht gemäß Art. 5 Abs. 2 dem Prinzip der "Rechenschaftspflicht" (Accountability)

INTERNATIONALER DATENTRANSFER

gemäß Art. 44 ff. DS-GVO

GEHT SIE NICHTS AN? WAS IST MIT IHREN CLOUD-ANBIETER?

IHRE ROADMAP ZUR DS-GVO

Handeln Sie jetzt!

1. SCHNELLSTMÖGLICH:
   BESTANDSAUFNAHME

2. BIS MITTE 2017:
   ÄNDERUNGSBEDARF IDENTIFIZIEREN

3. BIS ZUM 25.05.2018:
   BEWERTUNG & UMSETZUNG DER VORGABEN

PSW GROUP

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT