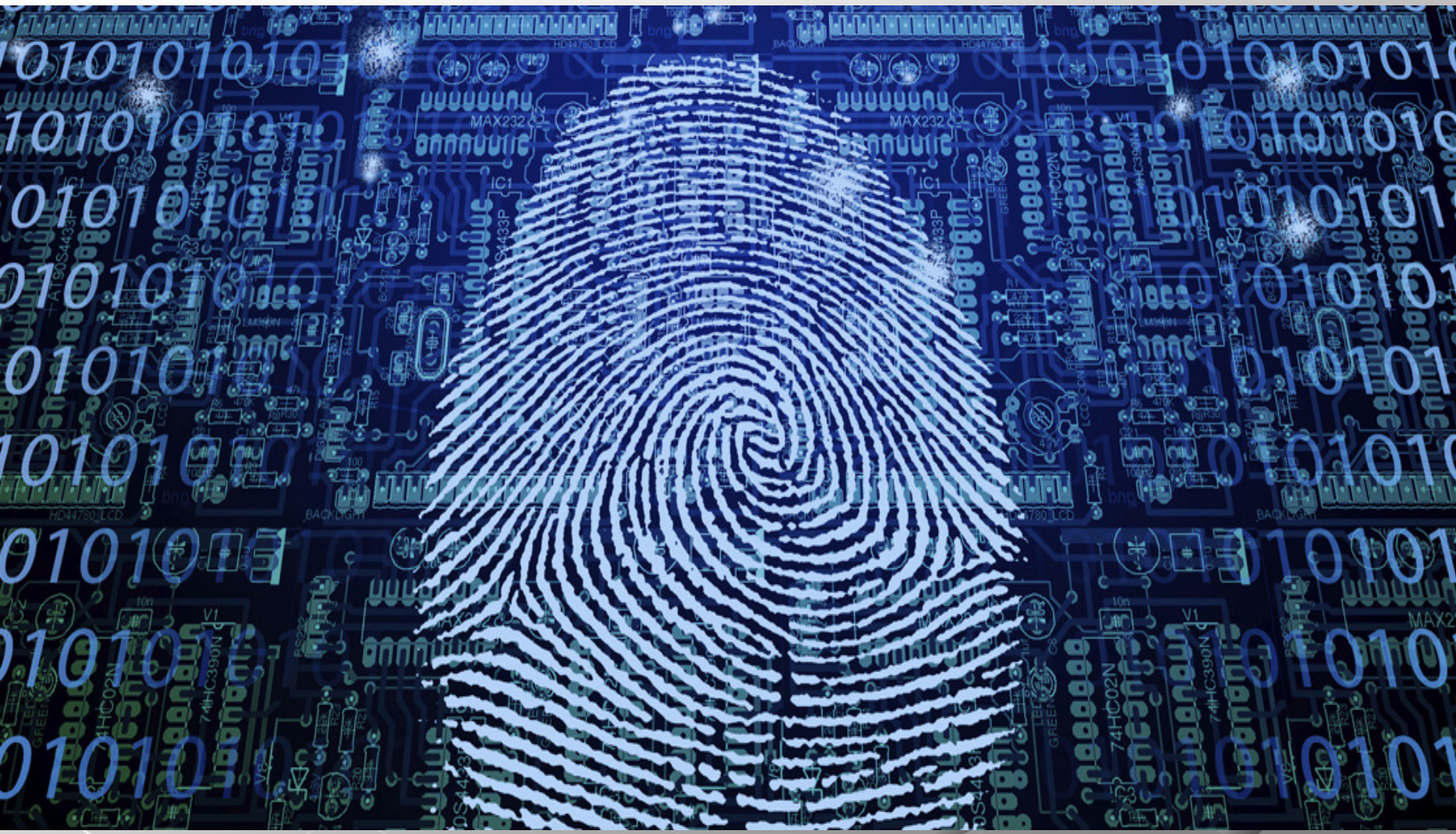
Die EU DSGVO 2018



RA Horst Speichert

© RA Speichert 2017

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Rechtsanwalt

Lehrbeauftragter
Universität Stuttgart

- Informationssicherheit
- Compliance-Audit
- IT-Verträge
- Betriebsvereinbarungen
- Datenschutz
- ext. Datenschutzbeauftragter
- EDV- und Internet-Recht
- Vorträge, Schulung, Seminare

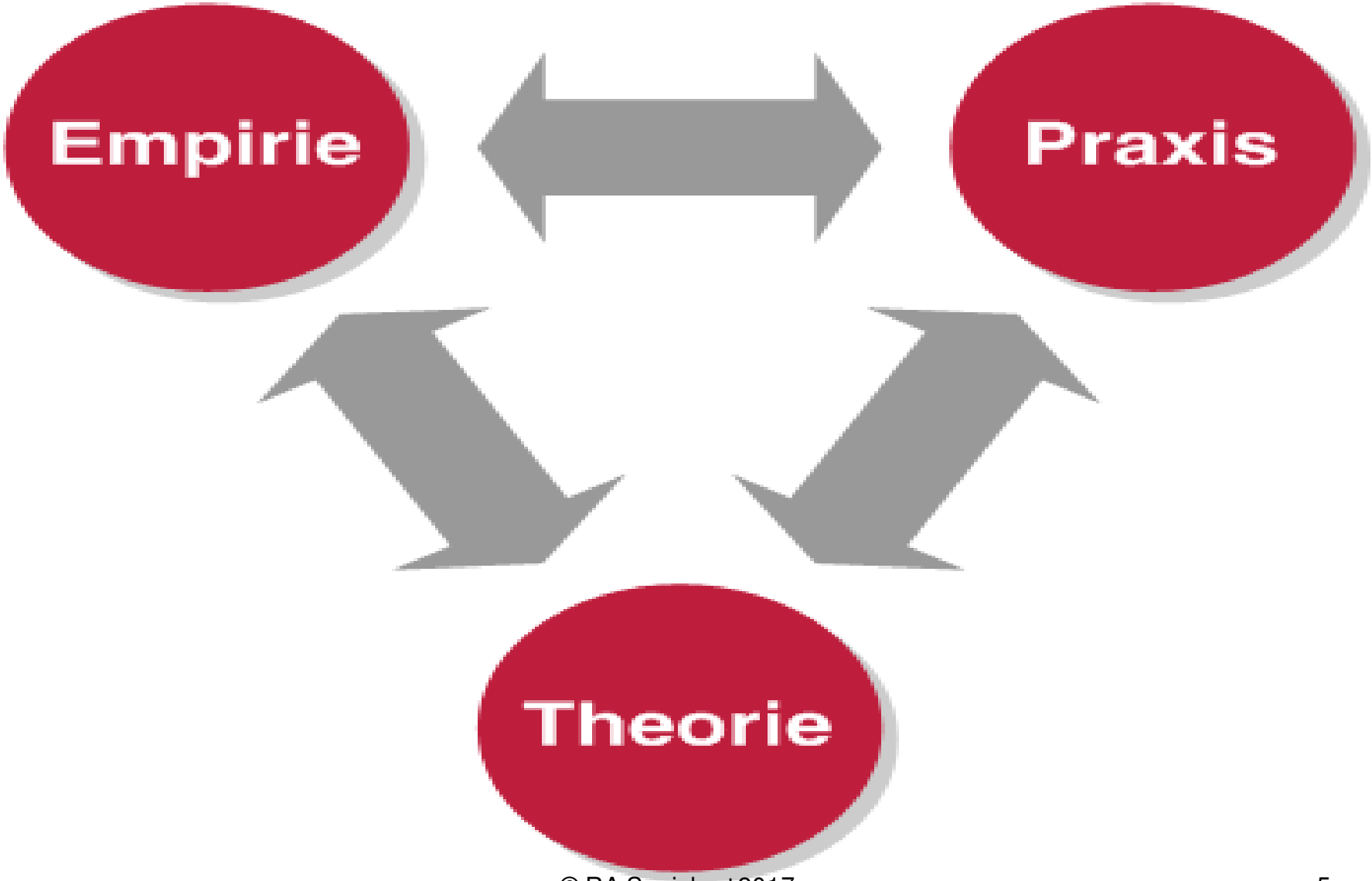
E-Mail: horst@speichert.de
Internet: http://www.kanzlei.de
http://www.speichert.de

Fit für die DSGVO?
Count-Down Praktische Umsetzung
Checkliste und Muster

Überblick

- **Anwendungsbereich**, Marktortprinzip
- Grundsätze, zentrale Definitionen
- Erlaubnistatbestände und **Einwilligungskonzept**
- **Auskunftsanspruch, Informationspflichten,** Widerspruchrecht
- **Recht auf Vergessen, Recht auf** Datenübertragbarkeit
- Privacy by design / Privacy by default
- **Auftragsdatenverarbeitung,** Datentransfer in Drittstaaten
- **Datenschutzerklärung,** standardisierte Symbole, Zertifizierung
- **Risikoansatz** statt Meldepflicht, **Datenschutzfolgenabschätzung**
- **Datenschutzbeauftragter, Aufsichtsbehörden,** One-Stop-Shop
- **Bußgelder** bis 4% des weltweiten Jahresumsatzes!
- Kollision mit deutschem Recht, was bleibt vom BDSG?
- wie geht es weiter? **Umsetzungsfrist** bis 2018
- **Checkliste**: notwendige Maßnahmen zur Umsetzung

Umsetzung im Unternehmen



Umsetzung der DSGVO

Vorgehensweise - Phasenplan

Bestands-aufnahme

- Überblick DSGVO
- Überblick neues BDSG
- vorhandene Unterlagen
- Fragenkataloge
- Gesprächs-Audit

Maßnahmen Roadmap

- allgemeine Checkliste
- Soll-Ist-Vergleich
- Gapanalyse
- individuelle Maßnahmen
- individuelle Roadmap

Zeitplan Umsetzung

- Zeitstrahl
- Dokumentation
- Ansprechpartner
- Delegation
- Netz von DS-Koordinatoren
- ToDo-Zeit-Matrix
- Freigabe Management

neues BDSG Stufenmodell

- DSGVO
- neue BDSG
- dynamische Anpassung
- Übersetzung englisch
- Einbindung Europa
- Einbindung weltweit

Überprüfung Schulung

- Schulungs-konzept
- Überprüfung
- Verbesserung
- PDCA-Konzept

Umsetzung der DSGVO

Umsetzungsfrist 25.05.2018

wie geht es weiter?

aktuelle Fassung

- Fassung vom 06.04.2016
- voraussichtlich finale Textfassung
- nach Veröffentlichung im Amtsblatt der EU am 25.05.16 in Kraft getreten

Umsetzungs-frist

- ursprünglich zwei Jahre Umsetzungsfrist bis zur Wirksamkeit der DSGVO
- also ab 25.05.2018

Umsetzung der DSGVO

5-Säulen-Modell

Verträge Drittstaaten

- ADV
- Verträge mit DL
- EU-Standard-V.
- BCR
- Arbeitsverträge
- BV

Dokumentation Risiko-management

- Verf.beschreib.
- Datenschutz-Folgenabschätzung
- Risikomanagement
- DSMS

Betroffenen-rechte Einwilligung

- Einwilligungen
- Cookies
- Informations-pflichten
- Auskunftsrechte
- Hinweispflicht Widerspruchsrecht

Organisation Schulung

- Schulung
- Konzern-DSB
- Meldepflichten
- genehmigte Verhaltensregeln
- Zertifizierung

IT-Sicherheit

- Datensicherheit
- toM
- Löschkonzept
- IT-Sicherheits-RL
- Videoüberwachung
- ISMS

© RA Speichert 2017

Anwendungsbereich

räumlicher Anwendungsbereich, Art. 3

- **räumlicher** Anwendungsbereich, **Marktortprinzip,** Art. 3
  - DV der EU-Niederlassung, unabhängig davon, ob die DV in der EU stattfindet
  - auch DV, die Personen in der EU nur betreffen; gilt auch für Auftrags-DV aus Drittstaaten
  - gleiche Wettbewerbsbedingungen in der EU, „Level Playing Field“

Marktortprinzip, Art. 3

Auslandsniederlassungen von EU-Firmen
Auch bei Verarbeitung außerhalb EU

Datenverarbeitung in der EU

Waren- und Dienstleistungsangebote für EU-Bürger

Monitoring
von EU-Bürgern

Verarbeitung nach Recht eines Mitgliedsstaates

© RA Speichert 2017

Sicherheit der Verarbeitung, Art. 32

Sicherheit der Verarbeitung, Art. 32

- § 9 BDSG wird in der bisherigen Form nicht mehr fortbestehen
- klassische Schutzziele der IT-Sicherheit: **Vertraulichkeit**, **Integrität, Verfügbarkeit,** Art. 32 Abs. 1
- **neu: Belastbarkeit** (resilience) der Systeme und Dienste, keine näheren Angaben zu konkreten Maßnahmen zur Belastbarkeit; gemeint ist Widerstandsfähigkeit, Erhalt der Funktionsfähigkeit trotz starker Belastung, z.B. durch DoS- oder DDoS-Attacken
- technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau bei Datensicherheit
  - **Stand der Technik**
  - **wirtschaftliche Verhältnismäßigkeit** → Berücksichtigung der Kosten
  - ausdrücklich genannt: **Pseudonymisierung** und **Verschlüsselung**
- **regelmäßige Überprüfung** der Wirksamkeit der Maßnahmen (Baseline-Ansatz, Soll-Ist-Vergleich, PDCA-Zyklus)

© RA Speichert 2017

Sicherheit der Verarbeitung, Art. 32

- Ermittlung **Schutzbedarf** der relevanten personenbezogenen Daten
  - **Risikobewertung,** Schadenspotential, z.B. normal, hoch, sehr hoch
  - für **Unternehmenswerte,** aber auch für **Rechte und Freiheiten** der betroffenen natürlichen Personen
  - Berücksichtigung der **Verarbeitungsrisiken** (z.B. Vernichtung, Verlust, Veränderung, unbefugte Offenlegung, unbefugter Zugang)
- gestiegene Bedeutung der IT-Sicherheit für DS-Verantwortliche
- **große Schnittmenge** mit IT-Sicherheit, Informationssicherheit, IT-Compliance → Synergien nutzen
- **Nachweis**, Art. 32 Abs. 3
  - z.B. durch **genehmigte Verhaltensregeln** gemäß Art. 40 oder genehmigtes **Zertifizierungsverfahren** gemäß Art. 42
  - **Rechenschaftspflicht** nach Art. 5 Abs. 2

Auftragsverarbeitung

Vergleich: altes Recht - neues Recht

- statt § 11 BDSG künftig Art. 28 DSGVO: zentrale Vorschrift für Auftragsverarbeiter in der DSGVO ist Art. 28
- Begriffe:
  - alt: Auftraggeber/Auftragnehmer
  - neu: Verantwortlicher/Auftragsverarbeiter
- Regelungen nach Art. 28 orientieren sich an der Systematik von § 11 BDSG, aber nun ausführlicher geregelt
- **Fiktion** bleibt:
  - nach BDSG: privilegierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 3 Abs. 8 Satz 3 und § 11 BDSG), wonach der per Auftrag eingesetzte Dienstleister **nicht Dritter** ist
  - Innenverhältnis ohne Prüfschranken, also kein gesonderter Erlaubnistatbestand für eine Datenübermittlung erforderlich

Vergleich: altes Recht - neues Recht

- findet sich in vergleichbarer Weise auch in der DSGVO: nach Art. 4 Nr. 10 ist ein **Auftragsverarbeiter nicht Dritter**
- aber keine Beschränkung der Privilegierung der Auftragsverarbeitung auf den EU-/EWR-Raum mehr, wie sich dies bisher aus der Eingrenzung in § 3 Abs. 8 Satz 3 BDSG ergab
- Auftragsverarbeiter können künftig also **auch außerhalb von EU-/EWR-Raum** sitzen (Marktortprinzip)

- aber: DSGVO auferlegt den Auftragsverarbeitern künftig **mehr Verantwortung und mehr Pflichten**

Kontrolle toM

- Verantwortlicher darf nur Auftragsverarbeiter einsetzen, die **hinreichend Garantien** dafür bieten, dass sie geeignete **technische und organisatorische Maßnahmen** für einen ausreichenden Datenschutz haben, Art. 28 Abs. 1
- **Umsetzung der Kontrollpflicht** beim Dienstleister
  - bei Beginn der Datenverarbeitung und sodann regelmäßig
  - bezüglich technisch-organisatorischer Maßnahmen
  - vor Ort? Problem bei Dienstleistern im Ausland
  - Dokumentenprüfung, Fragenkatalog, Gesprächsaudit
  - Zertifizierung
    - Zertifizierungsurkunde allein nicht ausreichend, eigene Prüfung erforderlich
    - Umfang (Scope), Zusammenfassung der Auditergebnisse

Kontrolle toM

- **neu** ist, dass der Auftragsverarbeiter gemäß Art. 28 Abs. 5 seine Verpflichtungen zur Einhaltung der toM nachweisen kann durch:
  - Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO (Code of Conduct)
  - eine Zertifizierung nach Art. 42 DSGVO

Subunternehmer

- **vorherige (schriftliche oder elektronische) Genehmigung**
- **allgemeine** Genehmigung des Verantwortlichen möglich
- spätere Änderungen bei Subunternehmen muss der Auftragsverarbeiter vorher mitteilen → Einspruchsmöglichkeit des Verantwortlichen
- kann keine Einigung erzielt werden, führt das zur Beendigung des Vertrags mit dem Auftragsverarbeiter

notwendiger Vertrag

- Auftragsverarbeitung auf der Grundlage eines für den Auftragsverarbeiter **rechtsverbindlichen Vertrags** oder eines anderen **Rechtsinstruments**
- wie bisher muss **im Regelfall ein Vertrag** über die weisungsgebundene Tätigkeit geschlossen werden
- **schriftlich** oder – neu - in **elektronischer Form,** Art. 28 Abs. 9 DSGVO
- für den notwendigen Inhalt des Vertrags gilt **weitgehend das Gleiche** wie bisher
- ein wichtiger Bestandteil: Darstellung der erforderlichen Sicherheitsmaßnahmen nach Art. 32 DSGVO

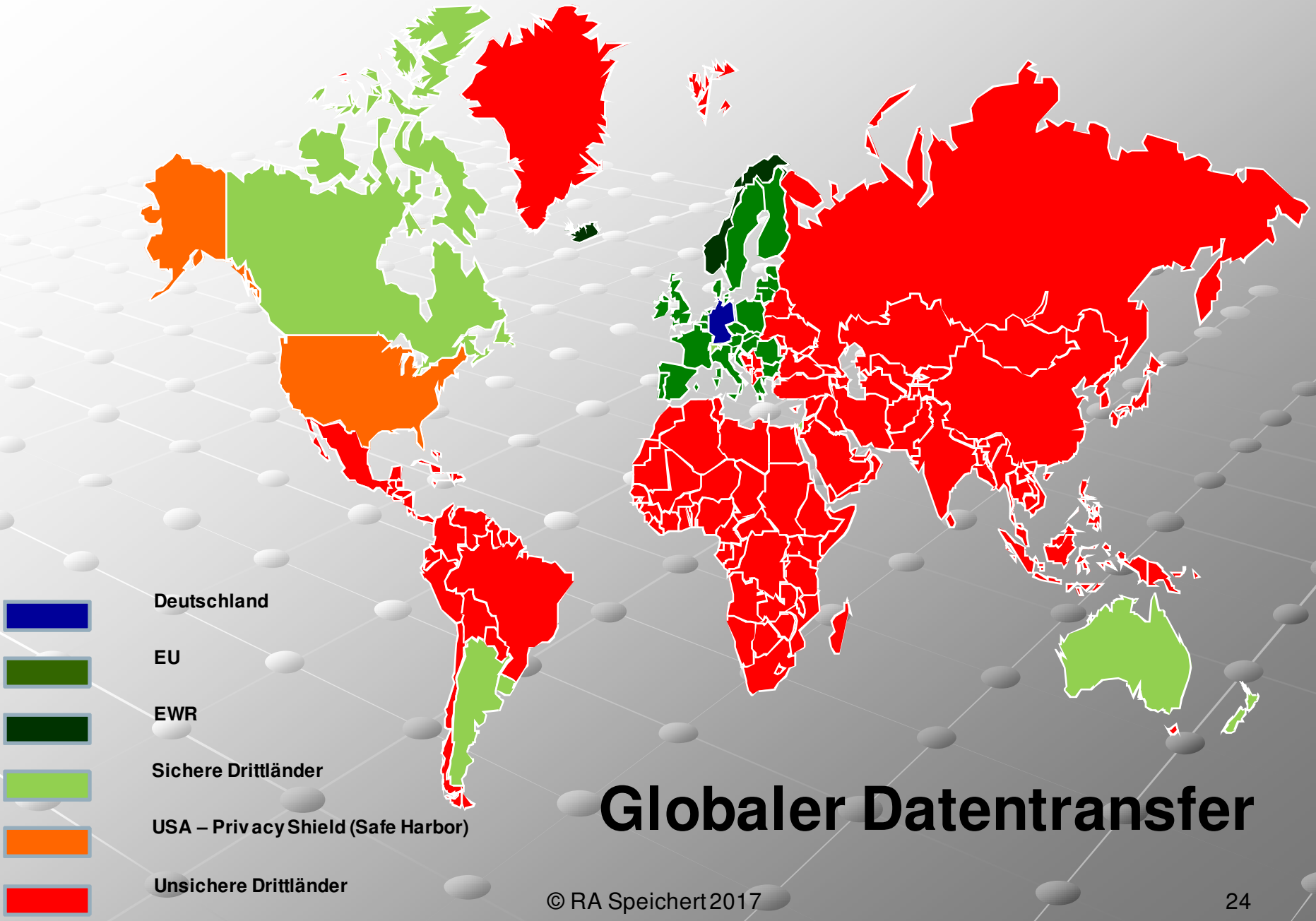
Pflichten Haftung/Auftragsverarbeiter

- **Verzeichnis** von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 muss auch Auftragsverarbeiter führen, muss der Aufsichtsbehörde auf Anfrage, z. B. bei Kontrollen, zur Verfügung gestellt werden
- bei Verstoß gegen Weisungen, z.B. bei Verarbeitung für eigene Zwecke oder Zwecke Dritter, gilt er nach Art. 28 Abs. 10 insoweit **selbst als Verantwortlicher,** mit allen rechtlichen Folgen, z. B. Erfüllung der Betroffenenrechte
- **Haftungsregelungen** bei Datenschutzverletzungen gelten nach Art. 82 DSGVO auch für Auftragsverarbeiter → Schadensersatzforderungen von Betroffenen
- **Meldepflicht bei Datenpannen:** Auftragsverarbeiter muss eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden, Art. 33 Abs. 2

Pflichten Haftung/Auftragsverarbeiter

- **Folgen bei Verstößen:** die umfassenden Bußgeldvorschriften des Art. 83 Abs. 4, 5 und 6 können auch bei Auftragsverarbeiter zur Anwendung kommen

Globaler Datentransfer



© RA Speichert 2017

Drittstaatentransfer

- Rechtsgrundlagen/Garantien des **angemessenen Datenschutzniveaus** für Drittstaatentransfers, Art. 46:
  - verbindliche Behördenabkommen (wie „Privacy Shield“)
  - Standarddatenschutzklauseln (bisher: Standardvertragsklauseln)
  - Verhaltensrichtlinien (Code of Conduct, CoC), Art. 40
  - Zertifizierungen, Art. 42
  - verbindliche Unternehmensregeln, Binding Corporate Rules (BCR), Art. 47
- Ausnahmen für notwendige Garantien, Art. 49:
  - Einwilligung oder Vertragserfüllung
  - öffentliches Interesse, Rechtsdurchsetzung
  - Schutz lebenswichtiger Interessen etc.

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- bisher bekannte Dokumentationen, § 4g Abs. 2, Abs. 2a BDSG
  - öffentliches Verfahrensverzeichnis und
  - interne Verarbeitungsübersicht (Verfahrensbeschreibungen)

werden mit der DSGVO abgelöst: **kein öffentliches Verzeichnis** und **keine Meldepflicht** (§ 4d, § 4e BDSG) mehr

- jetzt: schriftliches oder **elektronisches** Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten, Art. 30 Abs. 3
- wird in der Praxis notwendigerweise oft aus einer Reihe von **Einzelverzeichnissen** bestehen
- muss grundsätzlich jeder **Verantwortliche** (z.B. Unternehmen, Freiberufler, Verein) und **– neu (!) -** auch ein **Auftragsverarbeiter** erstellen und führen

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- **Ausnahmen**: Verantwortliche und Auftragsverarbeiter mit weniger als **250 Mitarbeitern,** Art. 30 Abs. 5, es sei denn,
  - **Risiko für die Rechte und Freiheiten** der betroffenen Personen (z. B. Scoring) und die Verarbeitung **nicht nur gelegentlich** erfolgt
  - oder **besondere Datenkategorien** gemäß Art. 9 Abs. 1 DSGVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten gemäß Art. 10
- muss **Aufsichtsbehörden** jederzeit **auf Anfrage** zur Verfügung gestellt werden, Art. 30 Abs. 4 DSGVO, EW Nr. 82
- **Rechtsfolgen bei Verstoß:** Geldbuße, Art. 83 Abs. 4 a

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- wird wie bisher **wesentliche Rolle** spielen, um datenschutzrechtliche Vorgaben überhaupt einhalten zu können
- nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherzustellen
- bislang unklar, in welchem Detailgrad die **technischen und organisatorischen** Maßnahmen im neuen Verzeichnis aufgenommen werden müssen
- **Muster-Vorlage** der Datenschutzaufsichtsbehörden

Datenschutz
Folgenabschätzung

Datenschutz-Folgenabschätzung, Art. 35, 36

- bei **voraussichtlich hohem Risiko** für die persönlichen Rechte und Freiheiten, bereits **vorab Abschätzung der Folgen** für den Schutz personenbezogener Daten
- insbesondere bei neuen Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, Art. 35 Abs. 1
- **Fallgruppen**, bei denen eine Folgenabschätzung **stets durchzuführen** ist, Art. 35 Abs. 3
  - Profiling
  - Verarbeitung besonders sensibler Daten
  - umfangreiche Videoüberwachung
- **Datenschutzbeauftragter** ist zu beteiligen, Art. 35 Abs. 2
- zeigt die Datenschutz-Folgenabschätzung ein verbleibendes hohes Risiko, muss **Datenschutzaufsichtsbehörde** konsultiert werden, Art. 36 Abs. 1
- ähnlich bisher: **Vorabkontrolle** nach § 4d Abs. 5 BDSG

Datenschutz-Folgenabschätzung, Art. 35, 36

- Inhalt **Datenschutz-Folgenabschätzung**
  - **allgemeine Beschreibung** der geplanten Verarbeitungsvorgänge
  - **Erfassung der konkreten Risiken** für Rechte und Freiheiten betroffener Personen, z.B. die Analyse der wirtschaftlichen Lage, des Aufenthaltsorts, des Gesundheitszustands, der persönlichen Vorlieben, der Zuverlässigkeit, des Verhaltens einer Person etc.
  - **Bewertung der Risiken** für Rechte und Freiheiten der Betroffenen

DS-Folgenabschätzung

Die Folgenabschätzung trägt den Rechten der Betroffenen Rechnung und enthält zumindest Folgendes:

- eine **systematische Beschreibung** der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
- eine Bewertung der **Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der **Gefährdung** für die Rechtsgüter der betroffenen Person und
- die zur Bewältigung der Gefahr geplanten **Abhilfemaßnahmen**, einschließlich **Garantien, Sicherheitsvorkehrungen und Verfahren**, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die gesetzlichen Vorgaben eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen wird.

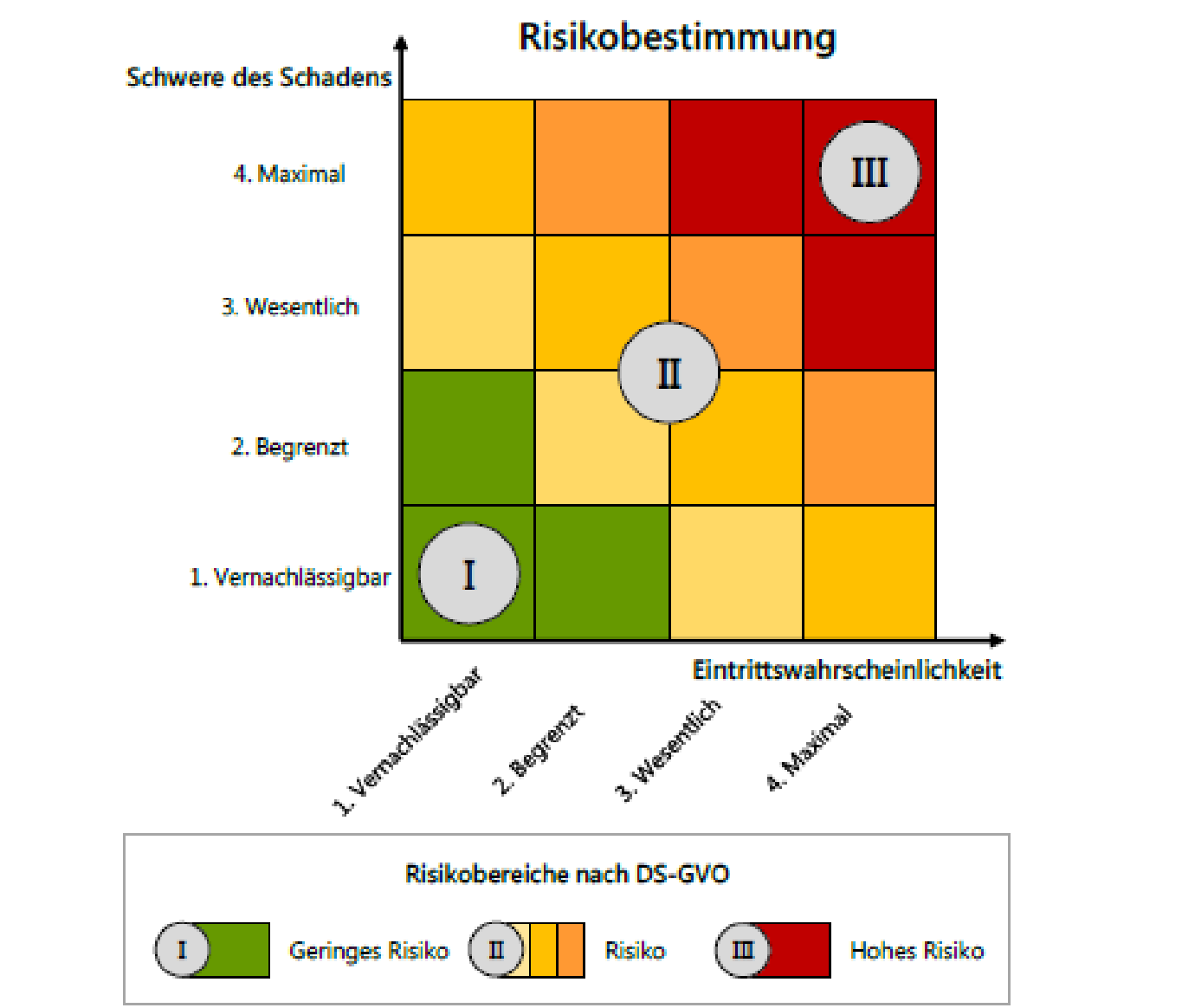
Risikobestimmung

- Risiko soll nach objektiven Kriterien ermittelt werden: Art, Umfang, Umstände und Zweck einer konkreten Verarbeitung, EW 76
- der Betroffene steht im Mittelpunkt der Betrachtung, nicht nur der (monetäre) Schaden für die Organisation (aber Triebfeder)
- dazu gehören Faktoren wie
  - **Eintrittswahrscheinlichkeit**
    - Risiko-Quelle, d. h. der „Angreifer“ muss bestimmt werden
    - technisch-organisatorische Schutzmaßnahmen
    - Umstände
  - **Schwere des Schadens**
    - hoher Schutzbedarf, z.B. aufgrund der Sensibilität z. B. bei Gesundheitsdaten
    - resultiert nicht zwangsläufig in ein hohes Risiko, z. B. bei geringer Eintrittswahrscheinlichkeit
    - Folgen für die Betroffenen

Folgen für die Betroffenen

- Schaden bezüglich „Rechte und Freiheiten“ der Betroffenen
- Verarbeitung kann zu physischen, materiellen und immateriellen Schäden führen, EW 75, darunter ist zu verstehen:
  - Diskriminierung
  - Identitätsdiebstahl
  - finanzieller Verlust
  - Rufschädigung
  - keine Kontrolle über eigene Daten
  - Profilbildung

Risikobestimmung - Risikomatrix



© Quelle: Bayrisches Landesamt für Datenschutzaufsicht, BayLDA

Risikoreduktion

- Risikoreduktion durch geeignete Maßnahmen
- Datenschutz-Maßnahmen (Privacy Controls): technische, organisatorische, rechtliche Maßnahmen
- sie ergänzen die Sicherheitsmaßnahmen nach Art. 32, die ohnehin durchzuführen sind

---

Ausblick

- Aufsichtsbehörden werden Listen von Verarbeitungstätigkeiten veröffentlichen, bei denen DSFA erforderlich ist (Positivliste, Whitelist) bzw. keine DSFA erforderlich ist (Negativliste, Blacklist)
- weiterführende Quellen:
  - ISO 29134, Privacy Impact Assessment
  - Privacy Impact Assessment der CNIL, franz. Datenschutzbehörde, https://www.cnil.fr/en/node/15798
  - auf europäischer Ebene: Working-Paper zur DSFA

Das neue BDSG

§

Das neue BDSG

- Kollision mit deutschem Recht, **was bleibt vom BDSG?**
- inoffizielle Referentenentwürfe, die nicht bestätigt wurden
  - Allgemeines Bundesdatenschutzgesetz (ABDSG) vom 05.08.2016
  - der zweite **inoffizielle Referentenentwurf** vom 11.11.2016 für die Ausführung/Ergänzung zur EU-Datenschutz-GVO wurde geleakt und am 23.11.16 ins Netz gestellt
- nun **offizieller Referentenentwurf** vom 01.02.2017 zur Anpassung des Datenschutzrechts, nachfolgend **BDSG-E**
- **Stellungnahme des Bundesrates** vom 10.03.17
- **Gegenäußerung der Bundesregierung** vom 23.03.17
- verabschiedet vom **Bundestag** in zweiter und dritter Lesung am 27.04.17
- **Bundesrat** hat Gesetzentwurf am 12.05.17 **zugestimmt**

Das neue BDSG

- **Bestellpflicht Datenschutzbeauftragter für Unternehmen,** § 38 BDSG-E, bisher § 4f BDSG
  - falls sie in der Regel **mindestens zehn** Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen
  - wenn sie **(risikobehaftete) Verarbeitungen** vornehmen, die einer **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO unterliegen
  - wenn sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten
- bisherige Regelungen **Scoring, Auskunfteien** bleiben im Wesentlichen bestehen
- **Bußgelder,** § 41 BDSG-E
  - nun Anwendbarkeit der Bußgeldhöhe nach DSGVO
  - für Verfahren wird auf das OwiG verwiesen
- **Strafvorschriften,** § 42 BDSG-E

Arbeitnehmerdatenschutz, § 26 BDSG-E

- bleibt national, Art. 88 Abs. 1; § 26 BDSG-E regelt den künftigen Beschäftigtendatenschutz
- entspricht weitgehend dem bisherigen § 32 BDSG
- Verarbeitung für Zwecke des Beschäftigungsverhältnisses
- **Kontrolle** zur Aufdeckung von Straftaten
  - nur **verdachtsabhängig**, sofern tatsächliche Anhaltspunkte
  - **Dokumentationspflicht**: tatsächliche Anhaltspunkte
  - Verhältnismäßigkeitsprüfung
- **Arbeitnehmer-Einwilligung**
  - **Freiwilligkeit** möglich, z.B. bei wirtschaftlichem Vorteil
  - **Schriftform**, soweit nicht wegen besonderer Umstände andere Form angemessen
- Verarbeitung **besonderer Kategorien personenbezogener Daten** bleibt möglich

Arbeitnehmerdatenschutz, § 26 BDSG-E

- **Betriebsvereinbarung** bleibt Erlaubnistatbestand, Art. 88 Abs. 1
- allerdings sind umfangreiche Anpassungen an DSGVO erforderlich
- Kollektivvereinbarungen (Betriebsvereinbarungen) sind Ermächtigungsgrundlage
- Rechte des **Betriebsrates** bleiben unberührt

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Rechtsanwalt

Lehrbeauftragter
Universität Stuttgart

- Informationssicherheit
- Compliance-Audit
- IT-Verträge
- Betriebsvereinbarungen
- Datenschutz
- ext. Datenschutzbeauftragter
- EDV- und Internet-Recht
- Vorträge, Schulung, Seminare

E-Mail: horst@speichert.de
Internet: http://www.kanzlei.de
http://www.speichert.de