complyit

DSGVO & Co:
Stolpersteine und Fallstricke bei der Umsetzung

Forum 7-it

München, 26. Februar 2018

Rainer Friedl
Rechtsanwalt, CISM (ISACA), DSB (TÜV)

Jean-Paul-Richter-Str. 41 • 81369 München
T: +49 (89) 38169810 • F: +49 (89) 381698109 • E: Rainer.Friedl@complyit.de

Rainer Friedl

Rechtsanwalt, CISM (ISACA), DSB (TÜV)

Rainer Friedl ist Rechtsanwalt und Berater für Datenschutz, Informationssicherheit und IT-Compliance. Er ist als Informationssicherheits-Manager (CISM) und Datenschutzbeauftragter (DSB TÜV) zertifiziert und verfügt neben seinen juristischen Fähigkeiten auch über vertiefte technische und organisatorische Kenntnisse und Erfahrungen bei der Informationsverarbeitung auf Grund seiner langjährigen Tätigkeit als Berater für IT-Infrastrukturen und System-Management.

Rainer Friedl betrachtet Datenschutz nicht als selbständige Unternehmensaufgabe, sondern als integrierten Teil der Informationssicherheit - natürlich mit seinen besonderen bzw. zusätzlichen Anforderungen. Seine Tätigkeitsschwerpunkte liegen in der Unterstützung von Unternehmen bei der Organisation und Steuerung der Informationssicherheit, bei der Prüfung und Optimierung von Prozessen und der technischen und organisatorischen Maßnahmen, bei der Durchführung von Risikobeurteilungen und Datenschutzfolgenabschätzung (DSFA) sowie bei Verhandlung, Ausarbeitung und Prüfung vertraglicher und organisatorischer Rahmenbedingungen wie z.B. Auftragsverarbeitung, internationaler Datentransfer, Policies und Richtlinien.

Außerdem hält Rainer Friedl Vorträge zu aktuellen Themen, führt Schulungen sowie Coachings durch und ist auch als Aufsichtsrat tätig.

DSGVO – Kurzer Überblick

Verarbeitung personenbezogener Daten nach der DSGVO

DSGVO ist direkt anwendbares EU-Recht

Einheitliche Geltung	• Keine nationalen „Ansichten“ • Aufsichtsbehörden haben keine „Deutungshoheit“
Erwägungsgründe	• Erwägungsgründe sind keine “Gesetzesbegründung” und erst recht kein Gesetz (Anhaltspunkte)
Keine Öffnungsklauseln	• Keine Möglichkeit eine andere Geltung herbeizuführen • Es handelt sich um Spezifizierungsmöglichkeiten

Bußgeld vielleicht nicht zentrales Sanktionsproblem: Schadensersatz, Art 82; Wettbewerbsrecht

- Schadensersatz und „Schmerzensgeld“ (immaterieller Schaden) nach amerikanischen Muster:
  Schadensersatz soll abschreckend wirken und weitere Verstöße unattraktiv machen

- Beweislastumkehr (Abs. 3): „… wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, …“

- Gesamtschuldnerische Haftung (Auftragsverarbeiter haftet für seine Verletzungen, aber dann direkt)

- Zunehmende Relevanz von Datenschutzverstößen im Hinblick auf Wettbewerbsverstoß (Marktverhalten regelnde Rechtsnormen)

Projektspezifische Umsetzungsprobleme

Umstellung DSGVO: Projektverzögerung

- Erstellung einer klaren Leitlinie zum Datenschutz als Unternehmensziel fehlt.
- Projekte zur Umstellung (Einführung) DSGVO sind finanziell und zeitlich oft zu knapp ausgestattet.
- Ressourcen (Spezialisten) sind nur bedingt verfügbar.
- Umstellungszeit 2 Jahre zu kurz?
  Renate Nikolay* (sinngemäß): Hätten wir 3 Jahre gegeben würden wir die gleiche Diskussion nächstes Jahr führen.

*Kabinettvorstand der EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung; Äußerung im „Dialog-Camp“ in München am 23.2.2018

Umstellung DSGVO: Projektfehler

- Fehlende Projektdefinition (Aufgaben, Ressourcen, Zuständigkeiten, …)
- Aufwand wird massiv unterschätzt.
- Falsche Projektziele:

  z.B.: „~~DSGVO konform werden~~“ (kein Ziel sondern Wunsch / nicht messbar)
  Möglicher Projektziele:

  „Implementierung eines DSMS“; „Minimierung von Verarbeitungsrisiken in …“
- Sichtweise als einmaliges „Datenschutz-Projekt“ und nicht als Einführungsprojekt für ein Management-System

Motivationen und Nutzen von Datenschutzprojekten und -prozesse …

- Maßnahmen schützen auch andere Unternehmenswerte (Assets)
- Prozessüberblick (Verarbeitungen) durch regelmäßige Kontrolle führt zu Wettbewerbsvorteilen
- Nutzung der Erfahrung des Rahmenwerks für andere Zertifizierungen
- Verhinderung negativer Unternehmenswahrnehmung
- Nachweis der Compliance als Voraussetzung für Aufträge
- Sicherheit von Daten als Marketingkriterium
- Bessere Einschätzung von Risiken für das Unternehmen
- Nachhaltiges Unternehmens-Management

… wenn Minimierung der
Compliance-Risiken nicht reichen sollte …

Verarbeitung und Dokumentation

Datenschutzgrundsätze - Art 5 DSGVO: Gilt für jede Verarbeitung!

Rechtmäßigkeit	• Rechtmäßigkeit, Art 6 DSGVO (Verbot mit Erlaubnisvorbehalt) • Verarbeitung nach Treu und Glauben; Transparenzgebot
Zweckbindung	• Eindeutiger Zweck: Festgelegt und legitim • Zweckänderung unter engen Voraussetzungen möglich (Art. 6, Abs. 4)
Datenminimierung	• Zweckangemessen und -erheblich • Beschränkt auf das Notwendige
Richtigkeit	• Sachlich richtig • Neuester Stand, sonst Löschung oder Berichtigung
“Speicherbegrenzung”	• Identifizierung nur möglich solange für Zweck notwendig
Datensicherheit	• Integrität, Vertraulichkeit • Art 32 DSGVO “Sicherheit der Verarbeitung” ist zentrale Norm

Rechtmäßigkeit, Art. 6 – Rechtsgrundlage: Für jede Verarbeitung erfoderlich!

Einwilligung	• Bedingungen, Art. 7 (Informationen, Widerruf) • Bei Kindern erst ab 16 Jahren im Rahmen des Art 8. wirksam
Vertragsdurchführung	• Vertragsdurchführung oder Anbahnung
Rechtliche Verpflichtung	• Verpflichtende Regularien zur DV von pbD (EU/Mitgliedsstaat) Steuer- und Sozialgesetze,
Lebenswichtige Interessen	• Hohe Hürde, geringer Anwendungsspielraum
Öfftl. Interesse/Gewalt	• Aufgaben müssen im öfftl. Interesse liegen oder hoheitliche Gewalt wurde übertragen
Berechtigtes Interesse	• Zur Durchführung des Geschäftszwecks erforderlich/notwendig, aber nur, wenn Interessen des Betroffenen nicht überwiegen

Rechtsgrundlagen der Verarbeitung, Art. 6 Abs. 1

Voraussetzung „erforderlich“	• „Erforderlich“ heißt nicht „Wünsch Dir was“
Mehrere Rechtsgrundlagen	• JA!

Verzeichnis der Verarbeitungstätigkeiten: Keine Option - Pflicht

Grenze 250 Mitarbeiter ist (fast) obsolet:

- "… Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der Betroffenen birgt …"
- Ohne Übersicht der Verarbeitungen können Aufgaben und Vorgaben des DSGVO nicht erfüllt werden

Rückgrat des Datenschutzmanagements

- Verzeichnis ist "Basis" der Datenschutzdokumentation
- Verzeichnis muss sinnvoll um die Dokumentationspflichten ergänzt werden …

Inhalt Verarbeitungsverzeichnis, Art. 30

Bedeutung des Art. 30

- Art. 30 konkretisiert Art. 5 Abs. 2
- Bußgeldproblematik: „großes“ bei Art. 5 oder „kleines“ bei Art. 30

Detailgrad?

- Prozesse: Art. 4 Nr. 2: „Verarbeitung“ jeden […] ausgeführten Vorgang oder **jede solche Vorgangsreihe**“
- Gestaltungsmöglichkeiten

Verarbeitungsverzeichnis Art. 30
Normativer Inhalt

- Kontaktdaten Verantwortliche(r); Vertreter; DSB
- Zweck der Verarbeitung
- Kategorien betroffene Personen
- Arten personenbezogener Daten
- Kategorien von Empfängern der personenbezogenen Daten (Offenlegung)
- Übermittlungen an Drittland/internationale Organisation
- Angaben zu technischen und organisatorischen Maßnahmen
- Löschfristen

Verarbeitungsverzeichnis Art. 30
Ergänzender Inhalt – mehr als sinnvoll …

- Dokumentation des Inhalts und der Einhaltung der Informationspflichten („Datenschutzhinweise“) (Art. 12, Art. 13, Art. 14)
- Rechtsgrundlage(n) der Verarbeitung
- Einwilligungserklärung (soweit als Rechtsgrundlage), Prozessbeschreibung zur Einwilligung und Widerruf
- Dokumentation zur Einhaltung der Datenschutzprinzipien (Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Sicherheit der Verarbeitung, Privacy by Design, Privacy by Default)
- Schutzbedarfsfeststellung / Risikoanalyse / Schwellenwertanalyse / DSFA
- Dokumentation der Interessenabwägung (Rechte und Freiheiten Betroffene gegen Interessen des verantwortlichen)
- Technische Dokumentation: Speicherorte, Übertragungsprotokolle, erforderliche Systeme/Anwendungen, etc.
- Erfolgte interne und externe Prüfungen/Auditierung
- Dokumentation der Einführung der Verarbeitung
- Ergänzungen bei Auftragsverarbeitung/Joint-Control:
  - Auswahlkriterium/Verfahren
  - Kontrolle und Prüfung / Überwachungsmaßnahmen
  - Vertragsbedingungen

… wegen den Dokumentationspflichten!

Grundlage	Nachweis von …
Rechenschaftspflicht Art. 5 Abs. 2	Einhaltung der Datenschutzgrundsätze
Rechtmäßigkeit, Art. 6 / Art. 8 (Kind)	Einwilligung (ggf. Alterverifikation; Eltern), Rechtsgrundlage
Besondere Kategorien, Art. 9	Ausdrückliche Einwilligung
Erhebung, Art 12; 13	Information an Betroffenen bei Erhebung oder Nutzung
Verarbeitung, Art. 24	Verarbeitung gemäß DSGVO; Risikobehandlung; Wirksamkeit
Privacy by Default/Design, Art 25	Risikobehandlung; Wirksamkeit
Gemeinsame Verarbeitung, Art 26	Vereinbarung der Zuständigkeiten
Auftragsverarbeitung, Art. 28	Vertrag, Vertraulichkeitserklärung, Weisungen, Einhaltung von Art. 32
Verarbeitung unter Aufsicht, Art. 29	Weisungen (Richtlinie!)
Sicherheit der Verarbeitung, Art. 32	Maßnahmen; Prozess zur Prüfung, Beurteilung, Wirksamkeit der Maßnahmen
DSFA/Konsultation, Art. 35 f	Dokumentation des Prozesses
Drittlandübermittlung, Art. 44 ff	**Geeignete Garantien!**
Ausübung Betroffenenrechte, Art. 12 ff	**Prozessbeschreibung; Erteilung/Mitteilung/Bearbeitung**
Datenschutzverletzungen, Art. 33	**Prozessbeschreibung, Verletzung, Meldung**
…	

Löschkonzepte und Löschanspruch: Wird wegen Komplexität oft vernachlässigt

- Umsetzung: Lückenhaftigkeit? Eher solide statt vollständig.
- Bestimmung/Bestimmbarkeit des Löschzeitpunktes und Dokumentation erforderlich, Art. 30 Abs.1 Satz 2 lit. f DSGVO
- Katalog von Verarbeitungen (Kundendaten

Auftragsverarbeitung

Auftragsverarbeitung

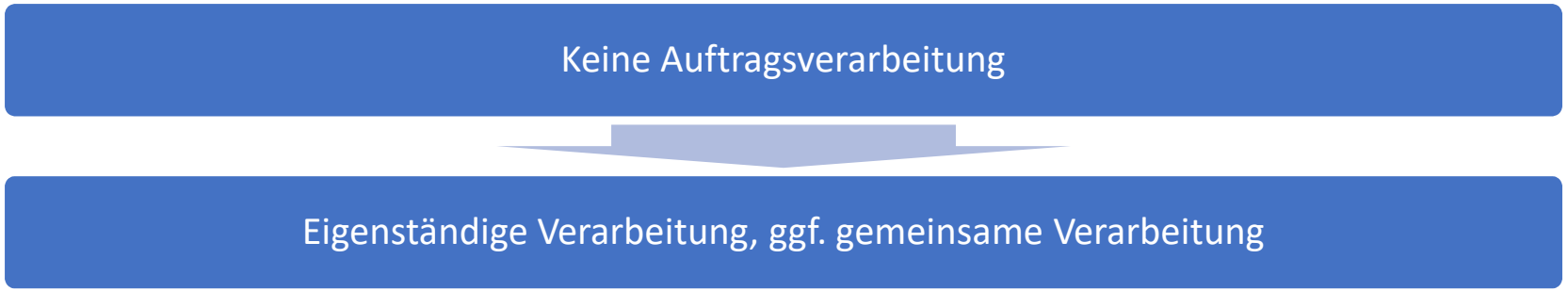
Form	• Schriftlich, wobei „elektronisches Format“ reicht • Achtung bei Verweis auf andere Vertragsgrundlagen mit Pflichtinhalt!
Unterauftragnehmer	• Gesonderte Genehmigung oder … • … Allgemeine Genehmigung mit Einspruchsmöglichkeit • Unklarheit bei Formvoraussetzungen
§ 11 Abs. 5 BDSG-alt Wartungsvertrag	• Nach deutschen Behörden: ähnliche Handhabung • Mal sehen ...
Privilegierung?	• hM: Keine gesonderte Rechtsgrundlage erforderlich

Auftragsverarbeitung: Abgrenzungsfragen

- Entscheidung über Zweck und Mittel der Verarbeitung (eigenverantwortliches Handeln, z.B. wenn Geschäftsbesorgung vorliegt).

- Rechtlicher oder tatsächlicher Einfluss auf die Entscheidung WOZU Verarbeitung erfolgt.

- Papier BayLDA: Kurzpapier Nr. 13 - Auftragsverarbeitung



Sicherheit der Verarbeitung

Schutzziele: Keine Erfindung der DSGVO

Vertraulichkeit

Art. 32 Abs.1 2.HS lit. b

- Konkretisierte Maßnahmen:
- Pseudonymisierung, Art. 32 Abs.1 2.HS lit. a
- Verschlüsselung, Art. 32 Abs.1 2.HS lit. a

Integrität

Art. 32 Abs.1 2.HS lit. b

- Keine Konkretisierungen im Gesetzestext

Verfügbarkeit

Art. 32 Abs.1 2.HS lit. b

- Konkretisierte Maßnahmen:
- Belastbarkeit der Systeme und Dienste, Art. 32 Abs.1 2.HS lit. b
- Verfügbarkeit der personenbezogenen Daten rasch wiederherzustellen, Art. 32 Abs.1 2.HS lit. c

Sicherheit der Verarbeitung (Art. 32 Abs. 1): Stand der Technik und Implementierungskosten

Stand der Technik?

- Mittelweg: Abgrenzung zu “Stand von Wissenschaft und Technik” und “(anerkannten) Regeln der Technik“
- Quellen: BSI (Mindeststandards für Behörden), Aufsichtsbehörden, Gutachten
- Dynamik: Regelmäßige Überprüfung erforderlich!

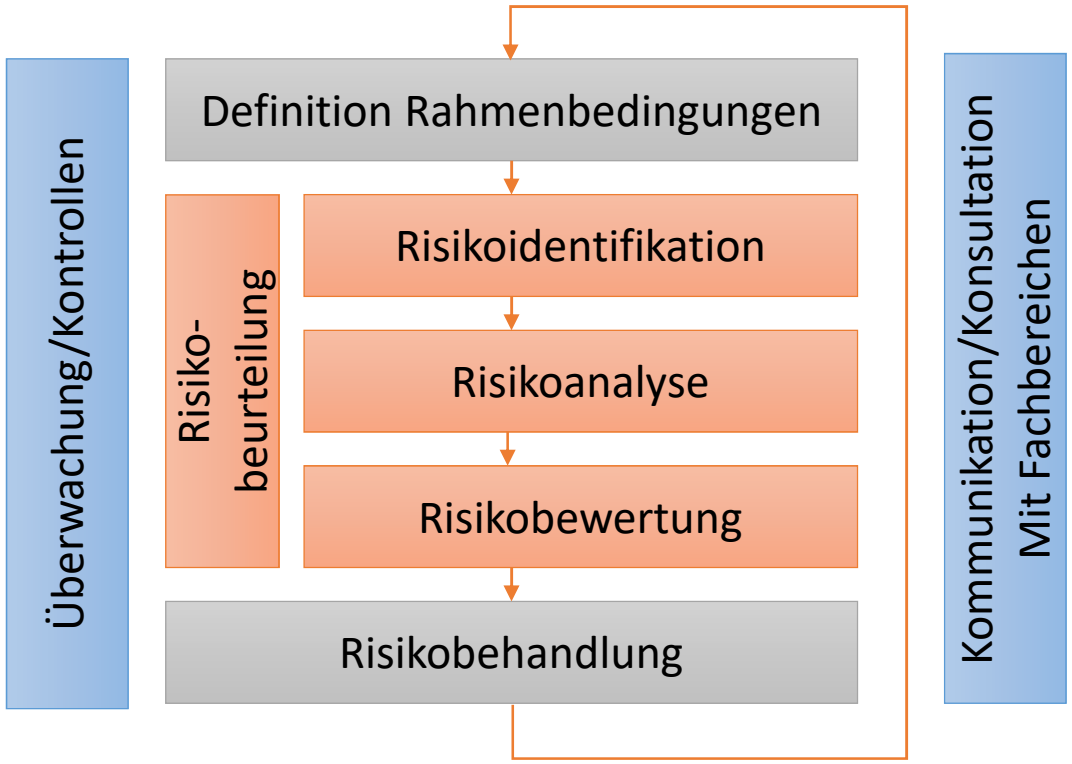
Implementierungskosten?

- Einbeziehung ökonomischer Aspekte für Verantwortlichen (Auftragsverarbeiter), ABER …
- „Zu teuer“ reicht nicht
- Abwägung muss getroffen werden (Begründung!)

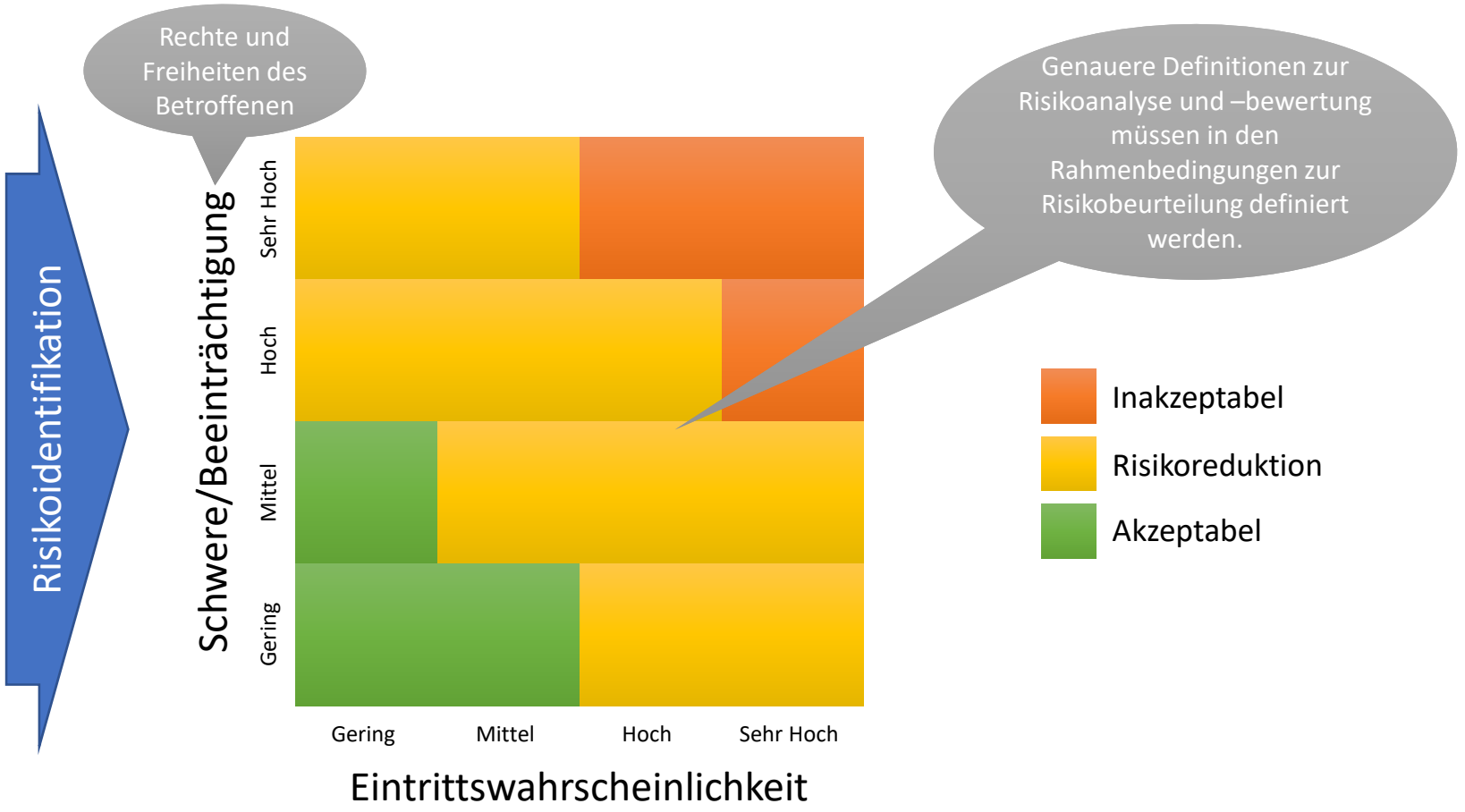
Risikofaktoren Art. 24, Abs. 1 (EG 75)

- Physischer, materieller oder immateriellen Schaden
  - Diskriminierung
  - Identitätsdiebstahl oder -betrug
  - Finanzieller Verlust, Rufschädigung
  - Verlust der Vertraulichkeit von Berufsgeheimnissen (pbD)
  - Unbefugte Aufhebung der Pseudonymisierung
  - Möglichkeit eines erheblichen wirtschaftlichen oder gesellschaftlichen Nachteils
- Beeinträchtigung der Rechte und Freiheiten
  - Beeinträchtigung der Rechte und Freiheiten
  - Hinderung der Betroffenen sie betreffende pbD zu kontrollieren
- Sensible Daten:
  - Verarbeitung von besonderen Daten (rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Zugehörigkeit zu einer Gewerkschaft, genetische Daten, Gesundheitsdaten, Sexualleben)
  - Daten zu strafrechtlichen Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln
- Profilerstellung: Bewertung (Betreffen, Analyse, Prognose) persönlicher Aspekte, insbesondere
  - Arbeitsleistung
  - wirtschaftliche Lage
  - Gesundheit
  - persönliche Vorlieben oder Interessen
  - Zuverlässigkeit
  - Verhalten
  - Aufenthaltsort oder Ortswechsel
- Schutzbedürftigkeit:
  - Verarbeitung pbD von schutzbedürftigen, natürlichen Personen, insbesondere Daten von Kindern
- Anzahl:
  - Verarbeitung großer Mengen an pbD
  - Große Anzahl von betroffenen Personen

DSGVO erfordert zwingend ein Risikomanagement



Ermittlung des Risikograde (Beispiel)



Risikobehandlungs-Methoden im Datenschutz:

Risikoakzeptanz	• Risikograd <= Risikokriterium • Vertretbares Restrisiko ist/wird erreicht
Risikominderung	• Risikograd > Risikokriterium • Auswahl von wirksamen Maßnahmen bis Risikoakzeptanz erreicht wird
~~Risikotransfer (Risikoübertragung)~~	• Risikograd > Risikokriterium • Teilung/Übertragung der Risiken: Dritter übernimmt Risiko oder Auswirkung (Outsourcing/Versicherung)
Risikovermeidung	• Risikograd >>>>>> Risikokriterium (Überschreitung) • Chance (Datenverarbeitung) wird nicht wahrgenommen oder ggf. neue konzipiert

Eine oder mehrere Optionen möglich

Datenschutzfolgenabschätzung und Konsultation

Verpflichtend bei HOHEM Risiko für Rechte und Freiheiten Betroffener

- Bewertungsmaßstäbe: Eintrittswahrscheinlichkeit und Schwere der Auswirkungen, Kontroll- und Minimierungsmaßnahmen
- Art 35 darf nicht isoliert gesehen werden, sondern eingebunden in den Risikomanagement
- "… Verwendung neuer Technologien …" meint Einführung einer für das Unternehmen neuen Technik (z.B. Feature-Update bei Software)

Muster-Fälle (Abs.3 nicht abschließende Aufzählung: "insbesondere")

- Rechtswirksame Entscheidung durch umfangreiche automatisierte Datenverarbeitung oder Bewertung persönlicher Aspekte
- Umfangreiche sensible Daten werden verarbeitet, Art.9 f (Ausnahmen beachten!)
- Opto-elektronische Vorrichtung Gegenstand des Verfahrens

Möglichkeit der Aufsichtsbörden von Positiv/Negativ-Listen

- Achtung: Entbindet nicht von der Durchführungsverpflichtung, wenn keine Listen erstellt werden!

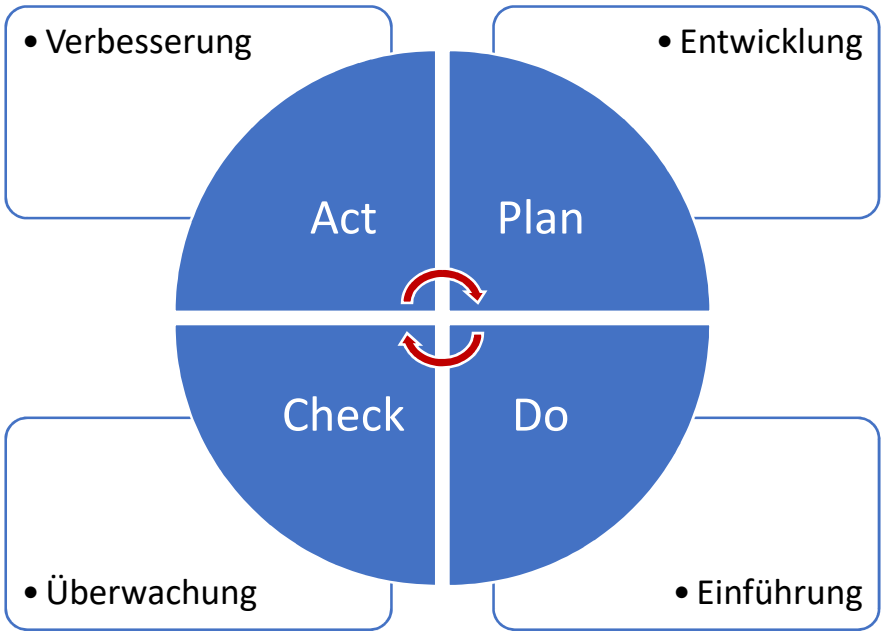
Konsultationsverfahren, Art. 37

- Spannender Gedanke: Hohes Risiko - keine Ahnung was man tun kann - will es aber trotzdem machen

Informationssicherheit: Sinnvolle, allgemeine Maßnahmen (Beispiele, nicht abschließend)

- Definition der Datenstruktur/Data Mapping und Verarbeitungs-Richtlinien
- Aktuelles Rechtekonzept (insbes. ‚Least-Privilege' auch im Admin-Bereich)
- Verschlüsselung der Kommunikation und bei Speicherung sensibler Daten
- Restriktive Konfigurationen (Privacy by Default)
- Backup und Desaster-Recovery Konzept
- Kompetente System-Implementierung und -Wartung
- Regelmäßige Softwareupdates sowie Ausmusterung veralteter Software
- Ggf. Sandbox Verfahren (z.B. BYOD)
- Verwendung/Analyse von Protokollierungen (SIEM)
- 2-Faktoren Authentifizierung (zumindest bei externem Zugriff)
- Zeitgemäße Firewall
- Monitoring und Schwachstellenanalyse
- Netzwerksegmentierung
- Malware Protection (2-Lines of Defense)
- Abschottung von Entwicklungs-, Test und Produktivumgebungen
- Mitarbeiter Kompetenzen und Sensibilisierung vorantreiben (Schulungen)

Der „klassische“ PDCA-Management-Prozess



- In DSGVO zur Wirksamkeitsprüfung gefordert: Art. 32 Abs.1 lit. d)
- Sollte auf alle Prozesse im Datenschutzmanagement angewendet werden

“Sicherheit ist keine Zustand, sondern ein Prozess”

Vielen Dank …

… für Ihre Aufmerksamkeit!

Noch Fragen?