DSGVO: Was bedeutet sie für Management, Datenschutz-/ Informationssicherheits-Beauftragte und IT-Abteilungen?

Forum 7-it

RA Rainer Friedl

München, 24. April 2017

Rainer Friedl

Rainer Friedl ist als Rechtsanwalt in den Bereichen IT-Recht, Datenschutz und IT-Compliance sowie als Berater für Informationssicherheit tätig.

Starke technische Expertise aus langjährigen Tätigkeit als IT-Berater für System-Management und Infrastrukturen eine.

Ganzheitlicher Blick auf die immer komplexer werdenden Infrastrukturen zur Informationsverarbeitung und den damit zusammenhängenden rechtlichen und technischen Problemstellungen für Unternehmen.

Rainer Friedl – Rechtsanwalt
Jean-Paul-Richter-Str. 41 • 81369 München
T: +49 (89) 38169810 • F: +49 (89) 381698109 • M: +49 (174) 9801784
E: Rainer.Friedl@complyit.de

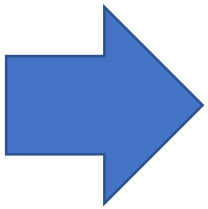
DSGVO – Einführung

DSGVO: Rechtsrahmen

- Am 25. Mai 2016 in Kraft getreten - am 25. Mai 2018 wirksam ohne weitere Übergangsfrist.
- Datenschutzrichtlinie 95/46/EG wird zum Wirksamwerden der DSGVO aufgehoben.
- Cookie-Richtlinie (2009/136/EG) bleibt in Kraft.
- E-Privacy-Richtlinie (2002/58/EG) wird nicht durch DSGVO aufgehoben, aber: EU-Privacy-VO vermutlich zum 25.5.2018 wirksam.

DSGVO: Eckdaten

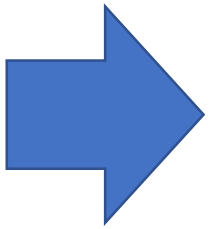
- Einheitliche Rechtsgrundlage in der EU (da VO)
  -> allerdings Öffnungs- und Ergänzungsklauseln
- Risikobasierter Ansatz
- Erweiterung der Dokumentationspflichten
- Ausweitung der Betroffenenrechte
- Bußgeldtatbestände erweitert; -höhe angehoben



Nicht, was wir uns gewünscht haben.
Aber damit lässt sich arbeiten.

DSGVO ./. DSAnpUG-EU

- „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“ liegt vor
- Wird wohl mit (ggf. wenigen Änderungen) verabschiedet
- Deutscher Gesetzgeber nutzt viele Gestaltungsräume („§ 5“-Ersatz in § 53 BDSGneu, DSB-Bestellung, Videoüberwachung)
- Aber auch viele Konkurrenzen und Erweiterungen (z.B. bei den Sanktionen: Privilegierung bei Erfüllung der Meldepflicht)
- Ziel der DSGVO war ein „einheitlicher Europäischer Standard“



Die vielfältigen Anpassungen und teilweise komplizierten Regelungen führen zu Rechtsunsicherheiten

DSGVO – Zentrale Themen

Verarbeitung personenbezogener Daten nach der DSGVO

Datenschutzgrundsätze - Art 5 DSGVO

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” geht deutlich weiter

Rechtmäßigkeit, Art. 6

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

Verantwortlichkeit des Verantwortlichen, Art. 24 Sicherheit der Verarbeitung, Art. 32

Treffen geeigneter Maßnahmen

- Ende des Regelungskatalogs zum § 9 BDSG
- Anpassung an IS-Ziele: Vertraulichkeit, Integrität, Verfügbarkeit, (Nichtabstreitbarkeit)
- Risikoabwägung!
- Konkretisierungen (z.B. Privacy by Design/Default, Art. 25)

Wirksamkeitsprüfung erfoderlich: PDCA-Zyklus (Art. 32, Abs.1,lit. d)

Verantwortliche und Auftragsverarbeiter gleichermaßen Adressat

Nachweis durch CoC (Art. 40) und Zertifizierungen (Art. 42) möglich

- Verhaltensregeln Versicherungswirtschaft werden wohl angepasst
- Privacy Impact Assessment: ISO/IEC 29134 ist im Verabschiedungs-Status

Datenschutzfolgenabschätzung und Konsultation Art. 35 f

Verpflichtend bei HOHEM Risiko für Rechte und Freiheiten Betroffener

- Bewertungsmaßstäbe: Eintrittswahrscheinlichkeit und Schwere der Auswirkungen, Kontroll- und Minimierungsmaßnahmen

MUSS-Fälle

- 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

Dritte bei der DV von pbD: Auswahl der richtigen Rechtsinstituts

Aufsicht des Verantwortlichen (Art 29)

- Regelmäßig „unterstellte“ Personen und Auftragsverarbeiter
- Anwendungsbereich für “Freelancer”? – Achtung: “Scheinselbständigkeit”

Gemeinsam Verantwortliche „Joint Control“ (Art 26)

- Bisher nach deutschem Recht unbekannt (RL nicht umgesetzt)
- Klare Definition der Aufgaben und Verantwortlichkeiten

Auftragsverarbeitung (Art 28)

- Ähnlich zu deutscher Regelung der ADV (§ 11 BDSG)
- Kein Raum mehr für “Funktionsübertragung” - Weisungsgebundenheit nicht notwendig für AV (bei ADV schon)
- Schriftlicher Vertrag und umfassende Dokumentation
- § 11, Abs. 5 BDSG fehlt!

Management

DSGVO: viele Dokumentationspflichten …
… explizit und implizit

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
…	

Datenschutzdokumentation
DS-Managmentsystem

"Rechenschaftspflicht" Art 5 Abs. 2
UND Dokumentationsverpflichtungen

Verantwortliche und Auftragsverarbeiter:
Umfassende Dokumentation aller datenschutzrelevanten Prozesse und Vorhaben notwendig.

Am besten "innerhalb" eines DS-Managementsystem (DSMS)

Verzeichnis der Verarbeitungstätigkeiten: Keine Option - Pflicht

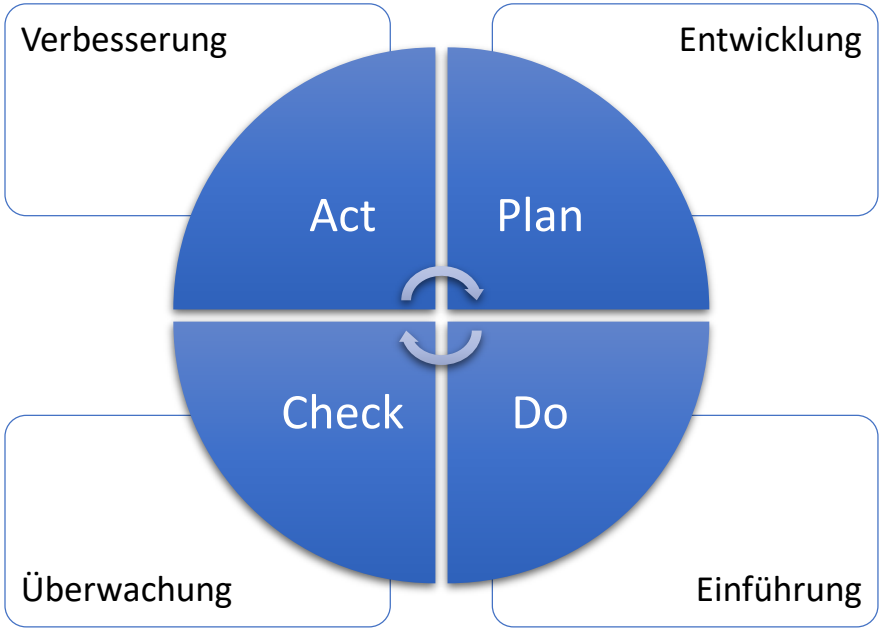
Grenze 250 Mitarbeiter ist (fast) obsolet:

- "… 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

Zentrale Übersicht

- Verzeichnis ist "Basis" der Datenschutzdokumentation
- Verzeichnis muss sinnvoll um die Dokumentationspflichten (s.o.) ergänzt werden

Der „klassische“ PDCA-Management-Prozess



- In DSGVO zur Wirksamkeitsprüfung gefordert: Art. 32, Abs.1,lit. d
- Sollte auf alle Prozesse im Datenschutzmanagment angewandt warden

“Sicherheit ist kein Zustand, sondern ein Prozess”

Risikobasierter Ansatz der DSGVO

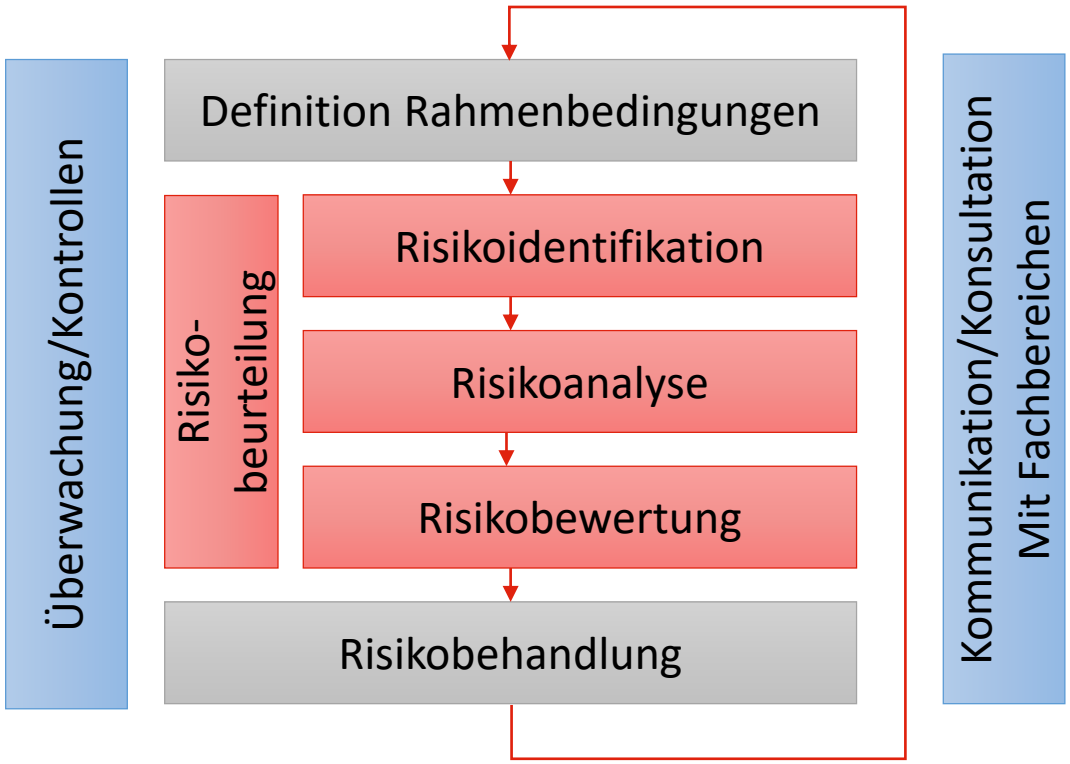
Risiken spielen eine erhebliche Rolle in der DSGVO:
Art. 24, 25, 32, 33, 34, 35, 36

Verantwortliche und Auftragsverarbeiter:
Einführung eines
datenschutzrechtlichen Risikomanagements

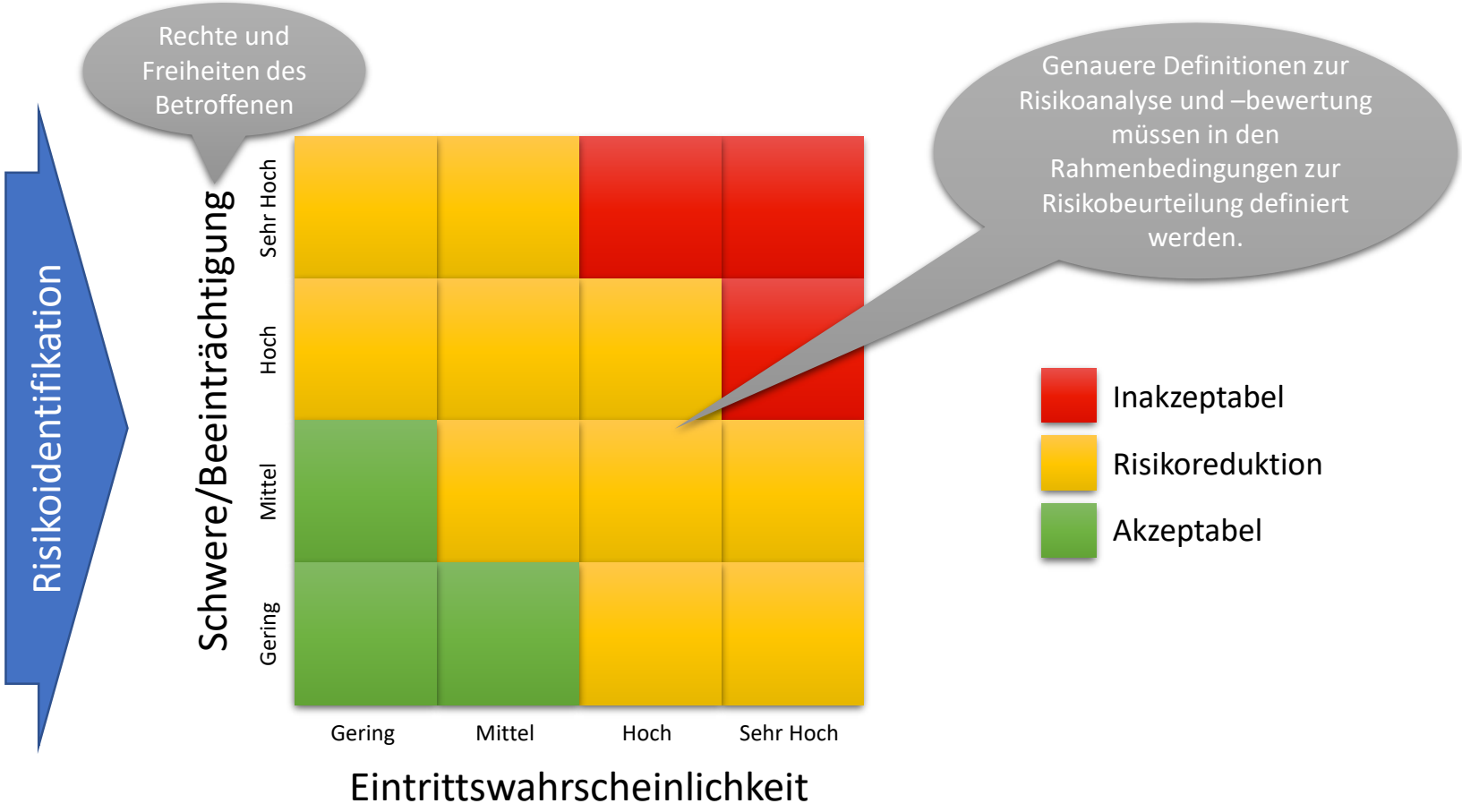
Risikofaktoren Art. 24, Abs. 1
Beispielkatalog (nicht abschließend) in Erwägungsgrund 75

- 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

Die Behandlung der Risiken erfordert zwingend ein Risikomanagement



Ermittlung des Risikogrades (Beispiel)



Risikobehandlungs-Methoden im Datenschutz:

Eine oder mehrere Optionen möglich

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 DV (Auftragsverarbeitung/Joint Control)
Risikovermeidung	• Risikograd >>>>>> Risikokriterium (Überschreitung) • Chance (Datenverarbeitung) wird nicht wahrgenommen oder ggf. neue konzipiert

Unternehmens-IT/IT-Abteilung

Bedeutung für IT-Abteilung:
Zentrale Maßnahmen mit Beteiligung der Unternehmens-IT

- 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
- 2-Faktoren Authentifizierung (zumindest bei externem Zugriff)
- 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)
- Zeitgemäße Firewall
- Monitoring und Schwachstellenanalyse
- Netzwerksegmentierung
- Malware Protection (2-Lines of Defense)
- Abschottung von Entwicklungs-, Test und Produktivumgebungen
- Mitarbeiter Kompetenzen und Sensibilisierung vorantreiben (Schulungen)

Bedeutung für IT-Abteilungen

Zentrale Rolle im “Maßnahmen-Paket”

- Der Unternehmens-IT kommt bei der Umsetzung von Maßnahmen eine Zentrale Rolle zu
- Dies betrifft auch Provider, Dienstleister, Berater, Systemhäuser, Softwarehersteller, Programmierer,

Anforderungen

- Insbesondere “Stand der Technik” erfodert eine permanente Prüfung
- Besondere Beachtung bei Beratungs- und Wartungsaufgaben

Handlungsbedarf

- Anpassung der Aufgabenbeschreibungen, Verträge und Strukturen
- Aufbau der teilweise gesteigerten Kompetenzanforderungen

Datenschutz-/ Sicherheitsbeauftragte

Datenschutzbeauftragter, Art. 37 ff: Erforderlichkeit, Formalien

- Pflicht zur „Bestellung“ wie bisher zu erwarten (BDSGneu), kann aber für kleine Unternehmen u.U. kompliziert werden:
  Unbestimmter Rechtsbegriff („umfangreiche Verarbeitung“)
- DSB oder eDSB mit Qualifikation, Fachwissen im DS-recht und DS-Praxis
- Konzernprivileg wurde berücksichtigt
- Keine Bestellungs-Formalität nach der DSGVO, allerdings schriftlich empfohlen: Aufgabenbeschreibung/Nachweis
- (Funktionale) Kontaktveröffentlichung und Mitteilung an Aufsichtsbehörde
- Personalunion mit Informationssicherheitsbeauftragten / (C)ISM/O?

Stellung des Datenschutzbeauftragten

Aufgabenkreis – mehr als „hinwirken“

- Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten
- Überwachung der Einhaltung der DS-Regularien
- Sensibilisierung und Schulung
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde

Deckung mit IS-Beauftragten?

- Große Schnittmengen, insbesondere bei den Maßnahmen
- Kompetenzbündelung (Risikomanagement, ISMS/DSMS)
- Zusätzlicher Schulungsaufwand, insbesondere “Recht”
- Faktische Stellung des IS-Beauftragten muss beachtet werden: Unabhängigkeit/Kontrollfunktion

Haftung des DSB

- Auf Grund der Aufgaben (Beratung/Überwachung) wird eine gesteigerte Haftung des DSB gesehen
- Direkthaftung ggü. Betroffenen eher nicht (vgl. Art. 82)

Fazit

Ergo:


DSGVO
Erheblicher Einfluss auf die Aufgaben für Management, Unternehmens-IT und Sicherheitsbeauftragte

Vielen Dank …

… für Ihre Aufmerksamkeit!

Noch Fragen?