UpDate! Datenschutz by Esturias

Die Datenschutz-Grundverordnung

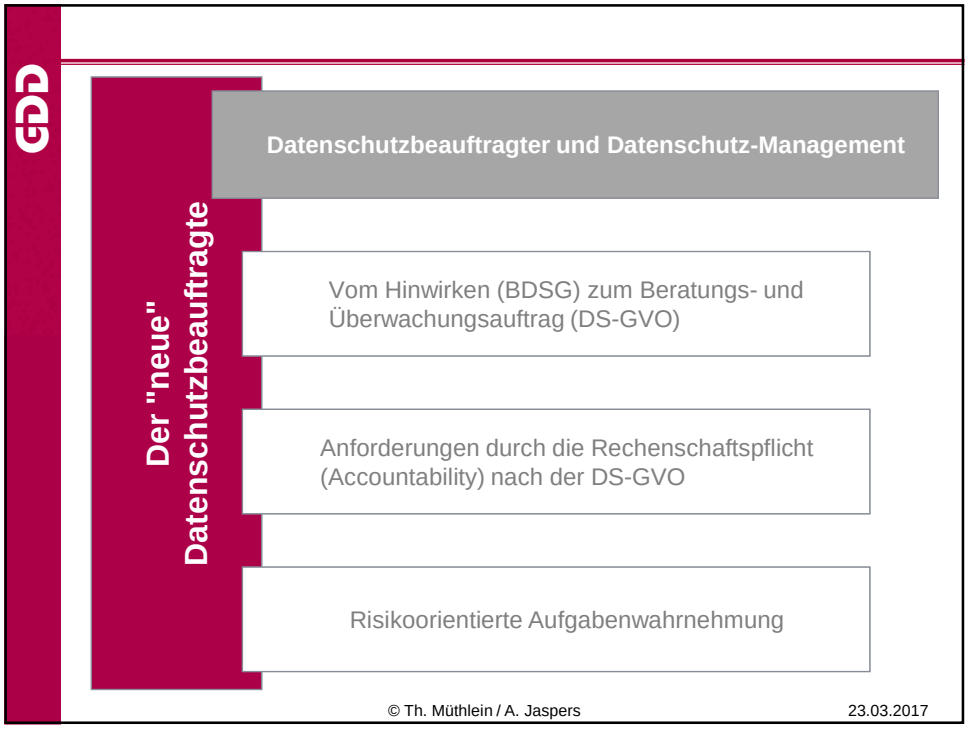
STELLUNG UND AUFGABEN DES BETRIEBLICHEN DATENSCHUTZBEAUFTRAGEN IM LICHTE DER EU-GVO

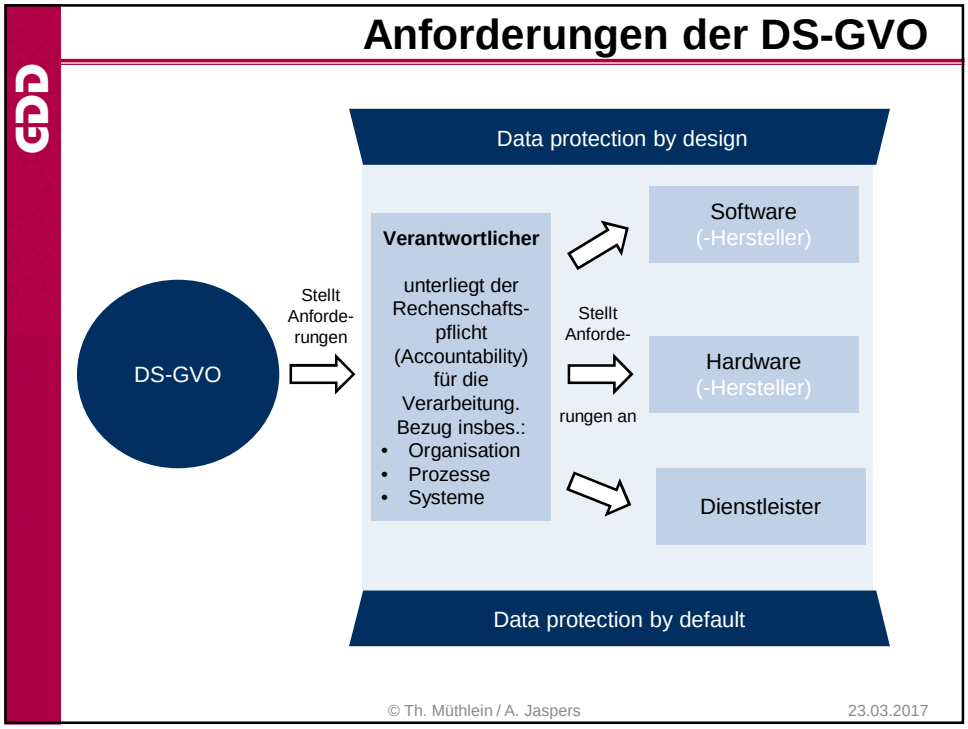
© Th. Müthlein / A. Jaspers 23.03.2017

Andreas Jaspers

- Rechtsanwalt
- Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn
- Referent der GDD-Datenschutz-Akademie
- Veröffentlichungen zu unterschiedlichen Aspekten des Datenschutzrechts und des Datenschutzpraxis
- Mitglied der Schriftleitung der Fachzeitschrift „Recht der Datenverarbeitung – RDV“
- Sachverständiger des Deutschen Bundestages zur Modernisierung des Datenschutzrechts (2007) und zum Beschäftigtendatenschutz (2009 und 2011)
- Sachverständiger des Landtages NRW zur Reform des Europäischen Datenschutzrechts (2013)

© Th. Müthlein / A. Jaspers 23.03.2017


Der "neue" Datenschutzbeauftragte
Datenschutzbeauftragter und Datenschutz-Management
Vom Hinwirken (BDSG) zum Beratungs- und Überwachungsauftrag (DS-GVO)
Anforderungen durch die Rechenschaftspflicht (Accountability) nach der DS-GVO
Risikoorientierte Aufgabenwahrnehmung
© Th. Müthlein / A. Jaspers
23.03.2017


Anforderungen der DS-GVO
Data protection by design
DS-GVO
Stellt Anforde-rungen
Verantwortlicher
unterliegt der Rechenschafts-pflicht (Accountability) für die Verarbeitung. Bezug insbes.:
• Organisation
• Prozesse
• Systeme
Stellt Anforde-rungen an
Software (-Hersteller)
Hardware (-Hersteller)
Dienstleister
Data protection by default
© Th. Müthlein / A. Jaspers
23.03.2017

Datenschutz-Organisation

Basis

- Datenschutzmanagementsystem, insbes. zur Gewährleistung der Accountability (geeignete Datenschutz-„Vorkehrungen" – engl.: approriate data protection policies), Art. 24 DS-GVO
  - Risikobasierter Ansatz
  - Überprüfung
  - Nachweis durch Zertifizierung möglich

Ergänzung

- Weitere Vorgaben zur operativen Datenverarbeitung insbesondere:
  - Einsatz „datenschutzfreundlicher" Technologien
  - IT-Sicherheit nach dem „Stand der Technik"
  - Weitrechende Dokumentationspflichten, u. a. aller Verarbeitungsvorgänge
  - Weitreichende Nachweispflichten insbes. nach dem Prinzip der Rechenschaftspflicht [accountability]
  - „Datenschutzfolgenabschätzung"
  - Konsultationspflicht der Aufsichtsbehörde

Normadressat ist der Verantwortliche (interne Organisation)

© Th. Müthlein / A. Jaspers 23.03.2017

Leitbild der DS-GVO zur Organisation des Datenschutzes

Leit-Thesen

1. Die DS-GVO setzt auf – etablierte – **Managementsysteme**, die bereits im BDSG angelegt sind, und schärft diese.
2. Art. 24 DS-GVO definiert die Organisationspflichten im Sinne des etablierten **PDCA (Plan–Do–Check–Act)-Zyklus**.
3. Grundsätzlich soll das Datenschutzmanagement/ die Datenschutzorganisation im Bereich der Unternehmensorganisation angesiedelt sein und ist **Aufgabe des gesamten Unternehmens**.
4. Die **Kontrolle** [engl. audit] des Datenschutzes in der Phase C - Check ist durch das Unternehmen intern sicherzustellen (z. B. Internes Kontrollsystem (IKS), Compliance-Organisation).
5. **(Externe) Überwachung** [engl. monitoring] erfolgt durch die Aufsichtsbehörden oder (bei Zertifizierung/Verhaltensregeln) durch Auditoren - und auch durch die Betroffenen.
6. Durch **Datenschutzbeauftragte** muss die Organisation unterstützt (Beratung, Anknüpfungspunkt ist insbesondere die Phase P - Plan) und überwacht werden, insbesondere im Hinblick auf die Funktionalität des internen Kontrollsystems.
7. Im Bereich der Überwachung stellt der Datenschutzbeauftragte zugleich auch eine eigenständige **ergänzende Überwachung** zur Aufsichtsbehörde dar.
8. Insbesondere die Überwachung durch den Datenschutzbeauftragten erfolgt **risikoorientiert**.
9. **Keine Garantenstellung des Datenschutzbeauftragten** besteht durch Beratung, insbesondere im Rahmen der Phase P - Plan – und die Überwachung, insbesondere in Anknüpfung an die Phase C - Check. Die (Umsetzungs-) Verantwortung im Rahmen des vollständigen PDCA-Zyklus liegt bei der verantwortlichen Stelle.

nach GDD-Praxishilfe DS-GVO II: Verantwortlichkeiten und Aufgaben nach der DS-GVO

© Th. Müthlein / A. Jaspers 23.03.2017

P – Plan:

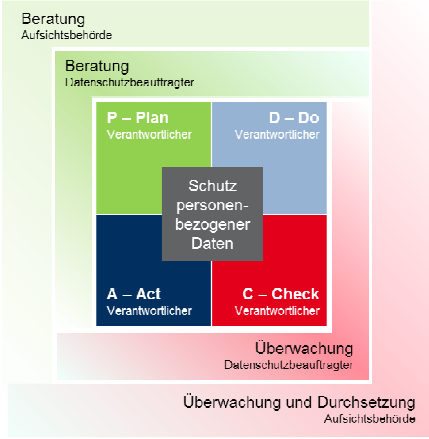
Planung + Konzeption

- Thema (an)erkennen
- Problem abgrenzen
- Ursachen identifizieren
- Ziel definieren
- Umsetzung planen

A – Act:

Optimierung + Verbesserung

- Erfahrung sichern
- Verbesserungspotenzial analysieren
- Verbesserungen initiieren



D – Do:

Umsetzung

- Umsetzung koordinieren
- Ergebnisse dokumentieren

C – Check:

Kontrolle

- Ergebnisse auswerten (ggf. inkl. Stichproben-Prüfungen)
- Soll-Ist-Analyse erstellen

Verantwortlicher = Verantwortliche Stelle/Unternehmen

© 2016 DATAKONTEXT GmbH – *aus: Gola/Jaspers/Müthlein/Schwartmann - Datenschutz-Grundverordnung im Überblick*

Datenschutzbeauftragter – Bestellpflicht

Verpflichtende Bestellung
(Art. 37)

- **Öffentliche Stellen**
- **Nicht-öffentliche Stellen (Unternehmen)**
  - *Kerntätigkeit besteht aus Verarbeitungsvorgängen, welche auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine **regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen*
  - *Kerntätigkeit besteht aus der **Verarbeitung besonderer Kategorien von Daten** gem. Art. 9, 10 DS-GVO in großem Umfang*
  - *Nach nationaler Regelung*

Verpflichtende Bestellung für nicht-öffentliche Stellen
(§ 38 BDSG)

- **Ergänzend** zu Art. 37
- **mindestens 10 Personen** ständig mit der automatisierten Verarbeitung beschäftigt (entspricht BDSG 2001) oder
- es werden Verarbeitungen durchgeführt, die einer **Datenschutzfolgenabschätzung** unterliegen oder
- bei **geschäftsmäßiger Verarbeitung**
  - zum Zweck der **Übermittlung** oder
  - zum Zweck der **anonymisierten Übermittlung** oder
  - für Zwecke der **Markt- oder Meinungsforschung**

Freiwillige Bestellung
(Art. 37)

- alle anderen Verantwortlichen

Aufgabenverteilung

Haupt-Aufgaben des **Unternehmens**	**Etablierung:** ▪ Datenschutz-Management (insbes. im Hinblick auf „Accoutability"/Nachweise) ▪ IT-Sicherheitsmanagement
Haupt-Aufgaben der **Fachabteilung, Mitarbeiter**	**Umsetzung:** ▪ Prozessgestaltung (Privacy by design/default) ▪ Datenschutzfolgenabschätzung/PIA ▪ Dokumentationen/Nachweise/Meldepflichten ▪ Prozesse für Rechte der Betroffenen
Haupt-Aufgaben der **IT**	**Umsetzung:** ▪ Vorgaben des IT-Sicherheitsmanagements **Unterstützung:** ▪ Technische Umsetzung der Datenschutzvorgaben in den Prozessen
Haupt-Aufgaben des **DSB**	**Beratung:** ▪ Abstimmung bei „Strategien" und – vorgegebenen – Einzelfällen **„Überwachung":** ▪ Umsetzung, risikoorientiert

© Th. Müthlein / A. Jaspers 23.03.2017

Verantwortlichkeiten im Einzelnen

Verantwortung des **Unternehmens**	Adressat: Leitung des für die Verarbeitung Verantwortlichen (Leitung des Unternehmens, AG-Vorstand, Vereinsvorstand, Geschäftsführung etc.)

- **Gesamtverantwortung** für den Datenschutz
- **Haftung:** Beweislastumkehr durch Nachweispflichten (Accountability) zu Lasten des Verantwortlichen
- **(Organisations-)Verantwortung** für die Umsetzung der DS-GVO insbes. mittels Anweisung bzw. Policies, ggf. Delegation an die Fachabteilung)
- Vermeidung des **Überwachungs**versagens durch Sicherstellung ordnungsgemäßer Überwachung der datenschutzrelevanten Unternehmensprozesse, insbes. Installation ausreichender Kontrollmechanismen und -systeme
- Einrichtung einer **Datenschutzorganisation**;
- Bereitstellung erforderlicher finanzieller, sachlicher und personeller **Ressourcen** zur Umsetzung sowie für die erforderliche Datenschutzorganisation
- **Bestellung** eines Datenschutzbeauftragten; Empfehlung der Installation eines „Datenschutzkoordinators"
- **Publizität** des Datenschutzbeauftragten

nach GDD-Praxishilfe DS-GVO II: Verantwortlichkeiten und Aufgaben nach der DS-GVO
so auch Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Verantwortlichkeiten im Einzelnen

Veranwortlichkeiten der **Fachabteilung, Mitarbeiter**

Fachabteilung

- Ausführung der **Anweisungen** der Unternehmensleitung zur Umsetzung der DS-GVO
- **Prozessverantwortung**; insbes. Definition der Schnittstellen (auch zum Datenschutz) und die Erfüllung von Dokumentationspflichten
- Vermeidung datenschutzrechtlicher Risiken durch **Prozess-, Produkt- und Technikgestaltung**, d.h. privacy by design/default, Löschkonzept usw.
- Erfüllung von **Transparenz- und Informationspflichten** sowie Gewährleistung der Betroffenenrechte
- arbeitsplatzbezogene **Instruktion** des einzelnen Mitarbeiters
- frühzeitige **Einbindung** des Datenschutzbeauftragten (erfolgskritischer Faktor)

Mitarbeiter

- **Vertrautmachen** mit internen Regelungen und ges. Vorschriften sowie Einhaltung derselben
- **Haftung**: ggf. persönliche Haftung gegenüber dem Arbeitgeber bzw. den Betroffenen; möglicher Adressat von Bußgeldbescheiden und möglicher Täter im Bereich des Datenschutzstrafrechts
- In datenschutzrechtlichen **Zweifelsfällen** stets den Datenschutzbeauftragten zurate ziehen

nach GDD-Praxishilfe DS-GVO II: Verantwortlichkeiten und Aufgaben nach der DS-GVO

© Th. Müthlein / A. Jaspers 23.03.2017

Verantwortlichkeiten im Einzelnen

Verantwortlichkeiten des **DSB**

- Adressatengerechte **Kommunikation** der Erforderlichkeit zur Anpassung an die kommende Gesetzeslage (DS-GVO) gegenüber Leitung und Fachabteilung
- **Hinwirkung** auf die Projektierung der Umsetzung der DS-GVO
- Unterstützung bei der Umsetzung und im laufenden Betrieb (**Beratungsauftrag**); Erläuterung und Präzisierung der gesetzlichen Anforderungen
- **Beratung** bezüglich Aufbau und Koordination eines Datenschutzmanagements
- **Monitoring** der Umsetzung der DS-GVO
- **Überwachung** der Einhaltung der gesetzlichen Vorgaben, der internen Vorschriften sowie der Funktionsfähigkeit des Datenschutzmanagements

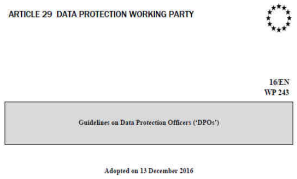
nach GDD-Praxishilfe DS-GVO II: Verantwortlichkeiten und Aufgaben nach der DS-GVO

© Th. Müthlein / A. Jaspers 23.03.2017

Bestellung

Anforderungen an die Bestellung:

- Berufliche Qualifikation, Fachwissen im Bereich Datenschutz-Recht und –Praxis und „Fähigkeit zur Erfüllung der in Art. 39 genannten Aufgaben"
- Benennung durch Verantwortlichen
- Veröffentlichung der Kontaktdaten (Funktionsbezogen)
- Meldung der Kontaktdaten an die Aufsichtsbehörde (Funktionsbezogen)
- Aufnahme des Namens und der Kontaktdaten in das Verzeichnis der Verarbeitungstätigkeiten


ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 243

Guidelines on Data Protection Officers ('DPOs')

Adopted on 13 December 2016

Zu Einzelheiten zum DSB s. auch schon

Artikel 29 Datenschutzgruppe – WP 243 v. 13.12.2016:

Guidelines on Data Protection Officers ('DPOs')

© Th. Müthlein / A. Jaspers 23.03.2017

Bestellung

Organisationen, die keinen DSB bestellen müssen oder freiwillig wollen, sind nicht daran gehindert, Personal oder externe Berater mit Aufgaben bezüglich des Schutzes personenbezogener Daten zu beschäftigen.

- Verantwortlichen und Auftragsverarbeitern wird empfohlen, die interne Prüfung, ob eine Bestellpflicht eines DSBs besteht oder nicht, zu **dokumentieren**, um nachweisen zu können, dass die einschlägigen Faktoren adäquat berücksichtigt worden sind.
- Wird ein DSB auf freiwilliger Basis bestellt, gelten **die Anforderungen der Art. 37 bis 39** wie bei der verpflichtenden Bestellung.
- Soweit kein DSB bestellt werden muss oder freiwillig wird können **Personal oder externe Berater** mit Aufgaben bezüglich des Schutzes personenbezogener Daten zu beschäftigen.
- Es darf in einem solchen Fall **keine Unklarheit** bezüglich ihres Titels, Status, Stellung und Aufgaben bestehen.
- Es ist bei jeder Kommunikation, insbes. mit Aufsichtsbehörden, Betroffenen und Öffentlichkeit klar zu stellen, dass es sich **nicht um einen DSB** handelt.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Interessenskonflikte

Die Organisation hat sicherzustellen, dass weitere Aufgaben und Pflichten des DSB nicht zu einem Interessenkonflikt führen

- Der DSB darf keine eine Position innerhalb der Organisation innehaben kann, die ihn dazu veranlasst, die **Zwecke und Mittel** einer Datenverarbeitung festzulegen (Beurteilung für jeden Einzelfall).
- Je nach Aktivitäten, Größe und Struktur der Organisation kann es als eine gute Praxis angesehen werden:
  - **Inkompatible Positionen** mit der Funktion des DSBs zu identifizieren
  - Interne Regeln zur der Vermeidung von **Interessenskonflikten** zu entwerfen
  - Eine **allgemeine Erklärung** über Interessenskonflikte zu integrieren
  - Zu erklären, dass der DSB keinen Interessenskonflikten bezüglich seiner Funktion als DSB unterliegt, um das Bewusstsein für diese Anforderung stärken
  - **Garantien** in den internen Organisationsregeln vorzusehen, die sicherstellen, dass die Stellenausschreibung für die Position des DSBs oder innerhalb des Dienstleistungsvertrags ausreichend präzise und detailliert ist, um Interessenskonflikte zu vermeiden. In diesem Zusammenhang sollte beachtet werden, dass Interessenskonflikte in Anhängigkeit von einer interner oder externen Beauftragung verschiedene Formen haben können.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Kontaktdaten des DSB

Betroffene sowie Aufsichtsbehörden müssen einfach, direkt und auf vertraulichem Weg den DSB kontaktieren können, ohne einen anderen Teil der Organisation kontaktieren zu müssen.

- Der Verantwortliche / Auftragsverarbeiter muss die Kontaktdaten des DSB **veröffentlichen** und sie an die zuständige **Aufsichtsbehörde kommunizieren**
- Die Kontaktdaten des DSB sollten es den Betroffenen und den Aufsichtsbehörden ermöglichen, den DSB auf **einfachem Weg zu erreichen** (eine postalische Anschrift, eine speziell eingerichtete Telefonnummer sowie eine speziell eingerichtete E-Mail Adresse).
- Ggf. können **andere Kommunikationsmittel**, z. B. eine speziell eingerichtete Hotline oder ein speziell eingerichtetes und an den DSB gerichtetes Kontaktformular auf der Webseite der Organisation zu Zwecken einer Kommunikation mit der Öffentlichkeit eingerichtet werden.
- Art. 37 Abs. 7 verlangt **nicht**, dass die Kontaktdaten **den Namen** des DSB beinhalten müssen, dies kann aber eine bewährte Praktik darstellen.
- Die Artikel-29-Datenschutzgruppe empfiehlt, dass die Aufsichtsbehörde und Beschäftigten über den Namen und die Kontaktdaten des DSB informiert werden (z.B. intern im Intranet, im internen Rufnummernverzeichnis, im Organigramm)

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Erreichbarkeit des DSB

Die Begrifflichkeit der Erreichbarkeit bezieht sich auf die Aufgaben des DSB als Kontaktstelle

- Es muss sichergestellt sein, dass die **Kontaktdaten** des DSB im Einklang mit den Anforderungen der DS-GVO verfügbar sind.
- Effiziente Kommunikation bedeutet, dass **diese Kommunikation in der Sprache**, die von der Aufsichtsbehörde und den Betroffenen verwendet werden, erfolgt.
- Gemäß Art. 37 Abs. 3 kann ein einzelner DSB für mehrere Stellen bestellt werden, wenn ihre **Organisationstruktur und Größe** berücksichtigt wird.
- **Organisationstruktur und Größe** müssen auch **bezüglich Ressourcen** und der Kommunikation Berücksichtigung finden. Ist er für eine **Vielzahl von Aufgaben** verantwortlich, ist sicherzustellen, dass der einzelne DSB diese effizient erfüllen kann, auch wenn er für mehrere öffentliche Behörden und Stellen zuständig ist.
- Die **persönliche Verfügbarkeit** des DSB ist essenziell (physisch auf demselben Betriebsgelände, mittels Hotline, anderer sicherer Kommunikationsmittel).
- Der DSB ist zur Wahrung der **Geheimhaltung** und der V**erschwiegenheit** verpflichtet.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

DSB auf Basis eines Dienstleistungsvertrags

Die Funktion des DSBs kann auf Basis eines Dienstleistungsvertrags (mit Einzelperson oder Organisation) ausgeübt werden.

- Bei einem Dienstleistungsvertrag mit einer Organisation muss jedes Mitglied dieser Organisation, das die Funktion des DSB wahrnimmt, alle einschlägigen **Anforderungen** von Abschnitt 4 der DS-GVO erfüllt (z.B. ist es essenziell, dass niemand einem Interessenskonflikt unterliegt).
- Jedes Mitglied muss unter dem **Schutz der Bestimmungen der DS-GVO** stehen (z.B. keine ungerechtfertigte Beendigung des Dienstleistungsvertrags hinsichtlich der Aktivitäten als DSB, aber auch keine ungerechtfertigte Kündigung eines einzelnen Mitglieds der Organisation, die die Aufgaben des DSBs ausführt).
- Es können individuelle Fähigkeiten und Stärken **kombiniert** werden, so dass verschiedene Individuen als Team ihren Kunden effizienter dienlich sind.
- Die **klare Zuweisung von Aufgaben** innerhalb des „DSB Teams“ sowie die Bestimmung eines Hautpverantwortlichen bzw. eines zentralen Ansprechpartners zu für jeden Kunden ist zu empfehlen.
- Diese Punkte sollten in einem **Dienstleistungsvertrag** festgelegt würden.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Weisungen und „in vollständiger Unabhängigkeit“

Art. 39 DS-GVO
EG 97

Es ist sicherzustellen, dass DSBs ihre Aufgaben mit ausreichenden Maß an Autonomie innerhalb ihrer Organisation ausüben können.

- DSB dürfen im Rahmen der Aufgabenwahrnehmung des Art. 39 DSBs **nicht instruiert** werden dürfen, wie sie mit einer Angelegenheit umgehen, z. B. welches Resultat erzielt werden soll, wie eine Beschwerde zu untersuchen ist oder ob die Aufsichtsbehörde zu konsultieren ist.
- Sie dürfen nicht instruiert werden, einen **bestimmten Standpunkt** hinsichtlich der Datenschutzgesetze einzunehmen, z. B. eine bestimmte Gesetzesinterpretation.
- Die Autonomie des DSBs bedeutet jedoch nicht, dass sie Entscheidungsbefugnisse außerhalb ihrer Aufgaben des Art. 39 haben.
- Der Verantwortliche / Auftragsverarbeiter bleiben für die Einhaltung der Datenschutzgesetze verantwortlich und müssen diese Einhaltung nachweisen können.
- Falls der Verantwortliche / Auftragsverarbeiter Entscheidungen treffen, die nicht mit der DS-GVO und dem Rat des DSBs im Einklang stehen, sollte dem DSB die Möglichkeit gegeben werden, seine abweichende Meinung klar gegenüber den Entscheidungsträgern äußern zu können

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Der "neue" Datenschutzbeauftragte

- Datenschutzbeauftragter und Datenschutz-Management
- **Vom Hinwirken (BDSG) zum Beratungs- und Überwachungsauftrag (DS-GVO)**
- Anforderungen durch die Rechenschaftspflicht (Accountability) nach der DS-GVO
- Risikoorientierte Aufgabenwahrnehmung

© Th. Müthlein / A. Jaspers 23.03.2017

Der DSB und seine Stellung nach DS-GVO – Vergleich zum BDSG

BDSG	DS-GVO
Fachkunde und Zuverlässigkeit	Berufliche Qualifikation, Fachwissen im Bereich Datenschutz-Recht und -Praxis und „Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben" Weitere Aufgaben möglich, soweit hierdurch kein Interessenskonflikt entsteht
Weisungsfreiheit bei der Ausübung der Fachkunde	Weisungsfreiheit bzgl. Aufgaben
Abberufungsschutz	Abberufungsschutz und Benachteiligungsverbot
Kündigungsschutz	(BDSG neu -nur soweit die Bestellung verpflichtend ist)
Unmittelbar der Unternehmensleitung unterstellt	Unmittelbarer Bericht an die höchste Managementebene
Verschwiegenheitsverpflichtung	Verschwiegenheitspflicht nach nationalem Recht
Unterstützungspflicht durch das Unternehmen	Unterstützungspflicht durch das Unternehmen: Erforderliche Ressoucen Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
Fortbildungsanspruch	Erhalt der Fachkenntnisse
Unterrichtungspflicht über „Vorhaben der automatisierten Verarbeitung personenbezogener Daten"	Ordnungsgemäße und frühzeitige Einbindung „in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen"
Recht zur Konsultation der Aufsichtsbehörde	Kontaktstelle zur / Zusammenarbeit mit Aufsichtsbehörde

Weitestgehend deckungsgleich!

© Th. Müthlein / A. Jaspers 23.03.2017

BDSG neu

§ 38 BDSG (2017 - E)	• Bestellpflicht
	• Verweis auf § 6 Abs. 4, Abs. 5 S. 2 und Abs. 6 (§ 6 Stellung eines Datenschutzbeauftragten öffentlicher Stellen)
§ 6 BDSG (2017 - E)	Abs. 4 (nicht bei freiwilliger Bestellung): • Abberufungsschutz • Kündigungsschutz
	Abs. 5 S. 2: • Verschwiegenheitspflicht
	Abs. 6: • Zeugnisverweigerungsrecht des Datenschutzbeauftragten und der ihm unterstellten Beschäftigten • Beschlagnahmeverbot

Entspricht der heutigen Rechtslage

© Th. Müthlein / A. Jaspers 23.03.2017

Aufgaben des DSB nach DS-GVO

Beratung

- Unterrichtung und Beratung hinsichtlich der Datenschutzpflichten (Verantwortlicher, Auftragsverarbeiter, Beschäftigte)
- Beratung Betroffener hinsichtlich der Datenschutzfragen/-rechte
- Beratung bei der Datenschutzfolgeabschätzung (auf Anfrage) (Pflicht des Verantwortlichen zur Konsultation gemäß Art. 35 Abs. 2 DS-GVO)

Risiko-orientierte Aufgaben-wahrnehmung

Überwachung

- Einhaltung DS-GVO und anderer Rechtsvorschriften
- „Strategien“ [engl. „Policies“], insbesondere hinsichtlich
  - Zuweisung von Zuständigkeiten
  - Sensibilisierung und Schulung der Mitarbeiter
  - Überprüfungen (zum Beispiel des internen Kontrollsystems)
- Durchführung der Datenschutzfolgeabschätzung durch den Verantwortlichen
- Zusammenarbeit mit der Aufsichtsbehörde/dem Ansprech-partner für die Aufsichtsbehörde

© 2016 DATAKONTEXT GmbH – *aus: Gola/Jaspers/Müthlein/Schwartmann - Datenschutz-Grundverordnung im Überblick*
© Th. Müthlein / A. Jaspers 23.03.2017

Der DSB und seine Aufgaben nach DS-GVO – Vergleich zum BDSG

BDSG	DS-GVO
Hinwirken auf die Einhaltung von Gesetzen und Vorschriften zum Datenschutz	Unterrichtungs- und Beratungspflichten (DS-GVO)
Mitarbeiterinformation	Accountibility → **Verantwortlicher!**
Vorabkontrolle bei kritischer Datenverarbeitung	Datenschutzfolgeabschätzung → **Verantwortlicher!** **Überwachung:** Durchführung der Datenschutzfolgeabschätzung
Verfügbarmachung des Verfahrensverzeichnisses für Jedermann	**Entfällt**
Hinwirken auf die Einhaltung von Gesetzen und Vorschriften zum Datenschutz	**Überwachung:** Einhaltung DS-GVO, anderer Rechtsvorschriften, „Strategien“
Überwachung der DV-Programme	**Überwachung:** Einhaltung DS-GVO, anderer Rechtsvorschriften, „Strategien“

Von der Hinwirkung zum Beratungs- und Überwachungsauftrag!

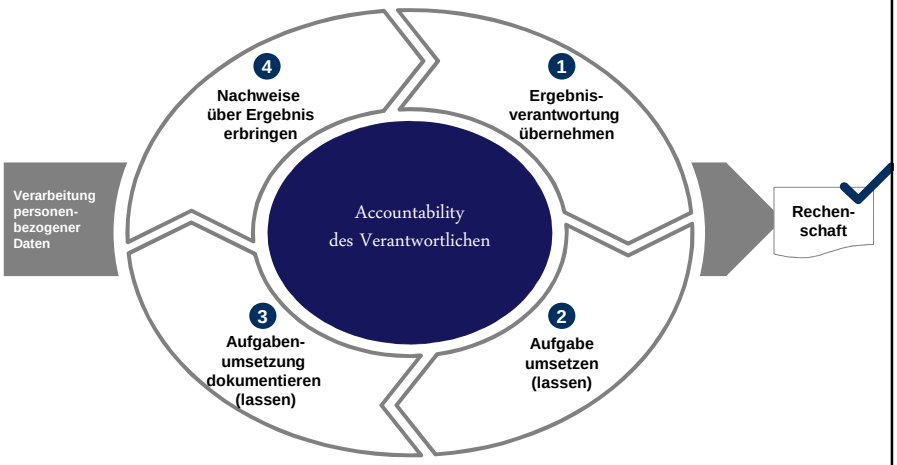
© Th. Müthlein / A. Jaspers 23.03.2017

Der "neue" Datenschutzbeauftragte

- Datenschutzbeauftragter und Datenschutz-Management
- Vom Hinwirken (BDSG) zum Beratungs- und Überwachungsauftrag (DS-GVO)
- **Anforderungen durch die Rechenschaftspflicht (Accountability) nach der DS-GVO**
- Risikoorientierte Aufgabenwahrnehmung

© Th. Müthlein / A. Jaspers 23.03.2017

Accountability

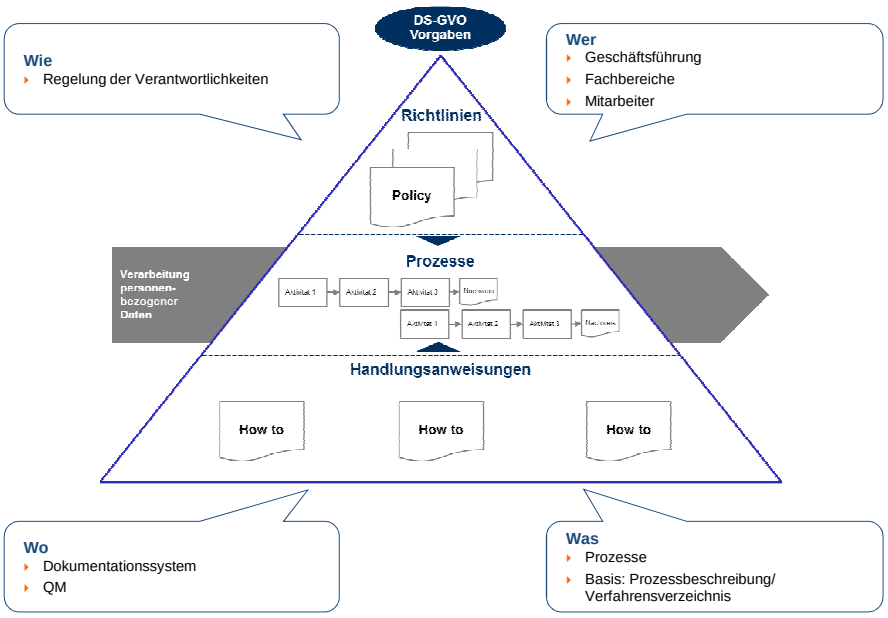


„Allgemein gesagt drückt er [gemeint ist der Begriff „Accountability"] ... aus, **wie Verantwortung überprüfbar wahrgenommen wird**. Verantwortung und Rechenschaftspflicht sind zwei Seiten einer Medaille und wesentliche Bestandteile der Good Governance."

Artikel-29-Gruppe, WP 173

© Th. Müthlein / A. Jaspers 23.03.2017

Implementierung (exemplarisch)



Wie
- Regelung der Verantwortlichkeiten

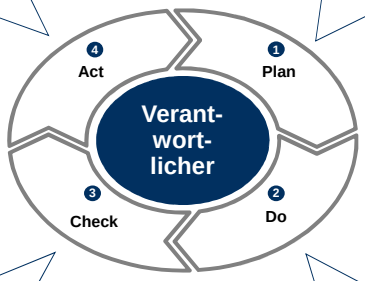
Wer
- Geschäftsführung
- Fachbereiche
- Mitarbeiter

Wo
- Dokumentationssystem
- QM

Was
- Prozesse
- Basis: Prozessbeschreibung/ Verfahrensverzeichnis

© Th. Müthlein / A. Jaspers 23.03.2017

Aufgaben des DSB im PDCA-Zyklus des Verantwortlichen (exemplarisch)



Optimierung – DSB:
- Beratung, z.B. Prozessvorgaben
- Überwachung, z.B. technisch-organisatorische Maßnahmen gemäß aktuellem Stand der Technik

Planung und Konzeption – DSB:
- Beratung, z.B. bei der Erstellung von Unternehmensrichtlinien (Policies) oder Prozessen
- Überwachung, z.B. bei Anfragen im Rahmen der Datenschutzfolgenabschätzung

Kontrolle und Überwachung – DSB:
- Beratung, z.B. Festlegung geeigneter KPI
- Überwachung, z.B. Erfüllungsgrad von DS-GVO-Nachweispflichten, ggf. stich-probenartige Kontrollen

Umsetzung – DSB:
- Grundsätzlich nicht involviert (Level 4 und 5 im Rahmen des operativen Geschäfts)
- Ggf. Unterstützung im Einzelfall

© Th. Müthlein / A. Jaspers 23.03.2017

WP 243

Aspekt der Accountability:

Der Datenschutzbeauftragte ist so auszustatten, dass er seine Aufgaben ordnungsgemäß wahrnehmen kann

Konkretisiert durch Art. 29-Gruppe in WP 243 und Annex zu WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Überwachung durch den DSB

Der Verantwortliche wird bei der Überwachung der internen Einhaltung der Bestimmungen der Verordnung vom dem DSB unterstützt (s.a. EG 97)

Als Teil seiner Pflichten in Gestalt der Überwachung der Einhaltung darf der DSB insbesondere:

- **Informationen** sammeln, um Verarbeitungsaktivitäten zu identifizieren,
- die Gesetzmäßigkeit von Verarbeitungsaktivitäten **analysieren** und prüfen,
- den Verantwortlichen oder den Auftragsverarbeiter informieren, beraten und **Empfehlungen** aussprechen.

Achtung:

- Die Überwachung der Einhaltung bedeutet nicht, dass der DSB im Falle eines Verstoßes verantwortlich ist.
- Der Verantwortliche, nicht der DSB, ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen und den Nachweis der Rechtmäßigkeit zu erbringen
- **Die Einhaltung des Datenschutzes ist eine unternehmerische Verantwortung des Verantwortlichen, nicht des DSBs**.

© Th. Müthlein / A. Jaspers 23.03.2017

WP 243

Der Verantwortliche wird bei der Überwachung der internen Einhaltung der Bestimmungen der Verordnung vom dem DSB unterstützt (s.a. EG 97)

Die Datenschutzfunktion sind effektiv und mit ausreichenden Ressourcen in Bezug auf die ausgeführten Verarbeitungen auszustatten

Die Information und Konsultation sollte ein Standardverfahren im Rahmen der Unternehmensführung darstellen

Es ist die Aufgabe des Verantwortlichen, nicht des DSB, eine Datenschutzfolgeabschätzung falls erforderlich durchzuführen

Der Verantwortliche, nicht der DSB, ist verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen

© Th. Müthlein / A. Jaspers 23.03.2017

Ressourcen

Die Datenschutzfunktion sind effektiv und mit ausreichenden Ressourcen in Bezug auf die ausgeführten Verarbeitungen auszustatten

Die nachfolgenden Punkte sollten insbesondere beachtet werden:

- Aktive Unterstützung der Funktion des DSB durch das **obere Management** (so z.B. auf Vorstandsebene)
- Ausreichende **Zeit** für DSBs, ihre Pflichten zu erfüllen. z. B. durch
  - Festlegung eines **Prozentanteils** der Zeit für die Funktion des DSB (bei „Teilzeit“)
  - Priorisierung der Pflichten des DSB / **Arbeitsplan** zu
- Angemessene Unterstützung mit finanziellen **Ressourcen**, Infrastruktur (Räumlichkeiten, Einrichtungen, Ausstattung) und gegebenenfalls **Personal**.
- Offizielle **Kommunikation der Bestellung** des DSB an die Beschäftigten.
- Sicherstellung des notwendigen **Zugangs** zu anderen Funktionen.
- Regelmäßige **Fortbildungen**.
- Ggf. Einrichtung eines **DSB-Teams** (ein Datenschutzbeauftragter und sein/ihr Personal) mit klarer interner Struktur des Teams bzgl. Aufgaben und Pflichten eines jeden Mitglieds.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Einbeziehung des DSB

Die Information und Konsultation sollte ein Standardverfahren im Rahmen der Unternehmensführung darstellen

Folglich sollten Organisationen sicherstellen, dass beispielsweise:

- Der Datenschutzbeauftragte **regelmäßig zu Treffen** des oberen und mittleren Managements eingeladen wird
- Anwesenheit des DSB bei Entscheidungen bezüglich einer **Datenschutz-Folgenabschätzung**. Alle relevanten Informationen müssen dem DSB **zeitnah zur Verfügung gestellt** werden, zur Ermöglichung einer angemessenen Beratung.
- Der Meinung des DSB muss immer ein **gebührendes Gewicht** gegeben werden.
- Im Falle einer **Meinungsverschiedenheit** empfiehlt die Artikel-29-Datenschutzgruppe als bewährte Praxis die Gründe, warum dem Rat des DSB nicht gefolgt wird, zu **dokumentieren**.
- Der DSB muss unverzüglich im Falle einer **Verletzung des Schutzes personenbezogener Daten oder anderer Vorkommnisse** konsultiert werden.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Der DSB bei der Datenschutzfolgeabschätzung (DSFA)

Es ist die Aufgabe des Verantwortlichen, nicht des DSB, eine Datenschutzfolgeabschätzung falls erforderlich durchzuführen

Der Verantwortliche sollte den Rat des DSB insbesondere zu den folgenden Fragestellungen einholen:

- Ob eine Datenschutzfolgeabschätzung **durchzuführen** ist
- Mit welcher **Methodik** bei der Durchführung einer DSFA vorgegangen werden soll
- Ob eine DSFA in der Organisation durchgeführt wird oder ob diese **extern vergeben** wird
- Welche **Garantien** (einschließlich technisch-organisatorischer Maßnahmen) anzuwenden sind, um das Risiko für die Rechte und Interessen der betroffenen Personen zu mindern
- Ob eine DSFA ordnungsgemäß durchgeführt und ob ihre **Schlussforderungen** (ob die Verarbeitung fortgeführt werden soll und welche Garantien angewendet werden) im Einklang mit der DS-GVO stehen. (Falls dem Rat des DSBs nicht gefolgt wird, sollte ausdrücklich dokumentiert werden, warum der Rat nicht berücksichtigt wurde.)

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Führen von Aufzeichnungen

Der Verantwortliche, nicht der DSB, ist verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen

- Art. 39 Abs. 1 ist ein **Minimum von Aufgaben** des DSB
- Der Verantwortliche ist nicht daran gehindert, den **DSB** mit der Aufgaben des Führens eines Verzeichnisses von Verarbeitungsaktivitäten **zu betrauen**.
- Das Verzeichnis sollte als ein **Werkzeug** gesehen werden, dem **DSB** die Erfüllung seiner Aufgaben in Form der Überwachung der Gesetzmäßigkeit, dem Informieren und Beraten zu ermöglichen.
- Das Verzeichnis ist ein **Werkzeug**, das es dem **Verantwortlichen** und der Aufsichtsbehörde auf Anfrage ermöglicht, einen Überblick über alle Verarbeitungsvorgänge mit personenbezogenen Daten, die eine Organisation durchführt, zu erhalten.
- Es ist eine Grundvoraussetzung für eine Gesetzesmäßigkeit und ein effektives Mittel bezüglich der **Rechenschaftspflicht**.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Der "neue" Datenschutzbeauftragte

Datenschutzbeauftragter und Datenschutz-Management

Vom Hinwirken (BDSG) zum Beratungs- und Überwachungsauftrag (DS-GVO)

Anforderungen durch die Rechenschaftspflicht (Accountability) nach der DS-GVO

Risikoorientierte Aufgabenwahrnehmung

© Th. Müthlein / A. Jaspers 23.03.2017

Risikobasierte Aufgabenwahrnehmung

Beratung

- Unterrichtung und Beratung hinsichtlich Datenschutzpflichten (Zielgruppen: Verantwortlicher, Auftragsverarbeiter, Beschäftigte)
- Beratung Betroffener hinsichtlich Datenschutzfragen und -rechten
- Beratung bei Datenschutzfolgeabschätzung (auf Anfrage; Pflicht Verantwortlicher zur Konsultation)

Zielsetzung:

Wirksame Umsetzung der DS-GVO in

- der Organisation
- Prozessen
- Systemen

Überwachung

- Einhaltung DS-GVO und anderer Rechtsvorschriften
- „Strategien" [engl. „Policies"], insbesondere hinsichtlich
  - Zuweisung von Zuständigkeiten
  - Sensibilisierung und Schulung der Mitarbeiter
  - Überprüfungen (zum Beispiel des internen Kontrollsystems)
- Durchführung der Datenschutzfolgeabschätzung durch den Verantwortlichen
- Zusammenarbeit mit der Aufsichtsbehörde/ Ansprechpartner für die Aufsichtsbehörde

Zielsetzung:

Überwachung der wirksamen Umsetzung der DS-GVO in

- der Organisation
- Prozessen
- Systemen

Risiko-orientierte Aufgaben-wahrnehmung

Risikobasierter Ansatz – (sämtliche) Maßnahmen müssen risikoangemessen sein!

© Th. Müthlein / A. Jaspers 23.03.2017

Risikobasierte Aufgabenwahrnehmung

Der DSB hat bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen

- Der DSB hat seine Aktivitäten zu **priorisieren** und seine Anstrengungen auf Fragestellungen zu fokussieren, die **höhere Datenschutzrisiken** darstellen.
  - Die Überwachung der Gesetzmäßigkeit von Datenverarbeitungsvorgängen, die eine vergleichsweise **geringen Risikograd** haben, darf nicht vernachlässigt werden, sondern
  - es sollte eine Fokussierung primär auf Bereiche mit einem **höheren Risiko** erfolgen.
- Selektiver und pragmatischer Ansatz für DSBs bei **Beratung** hinsichtlich:
  - der geeigneten **Methode** für eine Datenschutzfolgeabschätzung
  - der Bereiche, die im Fokus eines internen / externen **Datenschutzaudits** stehen sollten,
  - der bereitzustellenden internen **Schulungsmaßnahmen**
  - der Beurteilung, für welche Verarbeitungsvorgänge der DSB mehr Zeit und **Ressourcen** aufwendet.

Art. 29 Gruppe, WP 243

© Th. Müthlein / A. Jaspers 23.03.2017

Risikobehandlung nach DS-GVO

Nachweise erbringen
- Nachweise für Maßnahmenumsetzung beibringen

Schutzbedarf feststellen
- „Assets" erfassen
- „Assets" bewerten
- Schutzbedarf für „Assets" festlegen

Maßnahmen festlegen
- Technisch-organisatorische Maßnahmen entsprechend Risikobewertung festlegen

Risiken bewerten
- Bewertungsmatrix festlegen
- Eintrittswahrscheinlichkeit festlegen
- Eintrittsauswirkungen festlegen
- Risikoklasse je „Asset" bewerten

© Th. Müthlein / A. Jaspers 23.03.2017

Risikoorientierte Priorisierung der Überwachung

Klassische Risikoklassifizierung, z. B. IT Sicherheit
Fokus: Risiken für das Unternehmen (Unternehmenssicht)

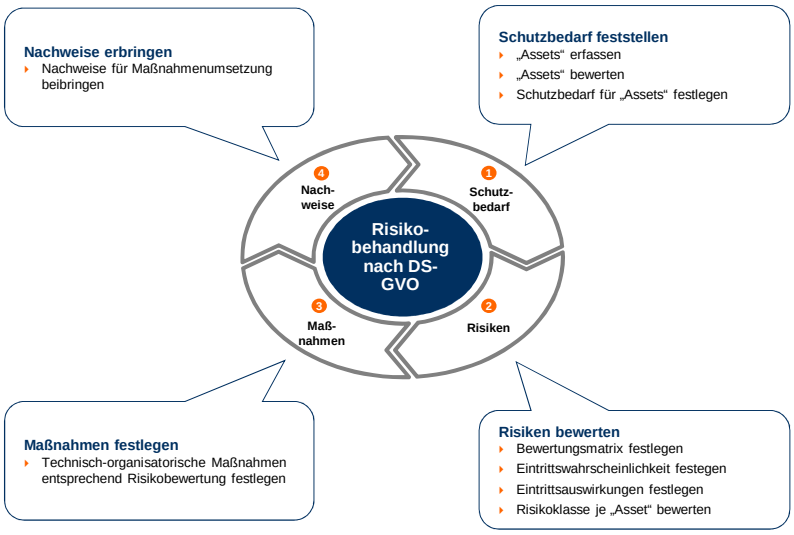
+

Risikoklassifizierung nach DS-GVO
Fokus: Risiken für Betroffenen (Betroffenensicht)

Risikoklassifizierung durch DSB zur Priorisierung seiner Überwachung
Fokus: Betroffenen- und Unternehmenssicht

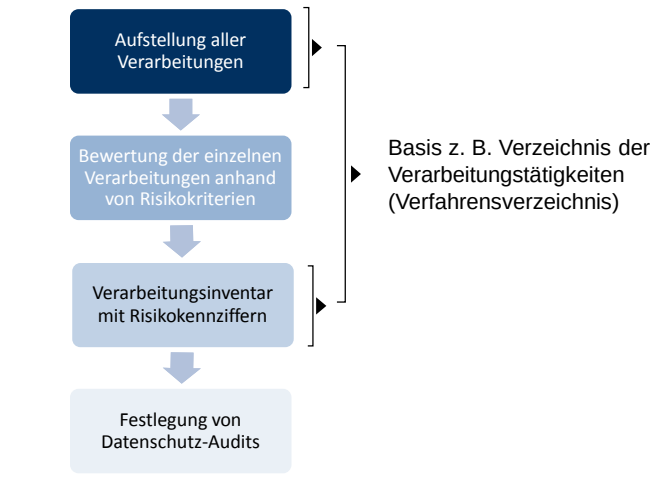
© Th. Müthlein / A. Jaspers 23.03.2017

Risikobehandlung nach DS-GVO



© Th. Müthlein / A. Jaspers 23.03.2017

Risikoorientierte Planung der Überwachung



© R. Herweg

© Th. Müthlein / A. Jaspers 23.03.2017

Beispiel einer Risikobewertung

Skala	1-10	1-10	1-10	1-10, 20	0, 1, 4, 7, 10	
Gewichtung	3	2	1	1	1	
Verarbeitung	Schutzbedarf der Daten	Komplexität der Verarbeitung	Prozess-immanente Risiken	Anzahl der Jahre seit letztem Audit	Ergebnis des letzten Audits	Risiko-Kennziffer
Verarbeitung 5	8	5	2	7	1	44
Verarbeitung 4	8	6	3	1	4	44
Verarbeitung 3	8	7	6	20	0	64
Verarbeitung 1	3	8	1	2	7	35
Verarbeitung 2	7	4	5	20	0	54
Verarbeitung 6	9	10	1	4	4	56

© R. Herweg

© Th. Müthlein / A. Jaspers 23.03.2017

Fazit und Thesen zum „neuen“ Datenschutzbeauftragten

1. **Stellung des DSB nach DS-GVO mit BDSG vergleichbar**
   - Stellung des DSB in der Organisation des Verantwortlichen entspricht weitgehend der Stellung nach BDSG, jedoch mit angepasstem Aufgabenfokus
2. **Aufgaben des DSB mit angepasstem Fokus**
   - Aufgaben verlagern sich vom „Hinwirken“ nach BDSG auf Beratungs- und Überwachungsauftrag
   - Aufgaben nach BDSG werden teilweise (entsprechend „Accountability“) auf den Verantwortlichen verlagert
   - Aufgabenwahrnehmung des DSB ist geprägt vom risikobasierten Ansatz
   - Aufgabenwahrnehmung muss Rechenschaftspflicht (des Verantwortlichen!) besonders berücksichtigen
3. **DSB verantwortet kein Tagesgeschäft**
   - Verantwortung des DSB beinhaltet nicht die operative Umsetzung durch andere Stellen in der Organisation des Verantwortlichen (Fachseiten/Abteilungen)
   - DSB berät/überwacht insbesondere auf den DSMS Leveln 2 (Richtlinien) und 3 (Prozesse) und bzgl. spezifisch zugewiesener Themenfelder

© Th. Müthlein / A. Jaspers 23.03.2017

Hilfsmittel zum Datenschutzbeauftragten

Hilfestellungen zum DSB nach BDSG (2001)

- GDD-Ratgeber „Der betriebliche Datenschutzbeauftragte“

Hilfestellungen zum DSB nach der DS-GVO

GDD-Praxishilfen DS-GVO:

- I - Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung
- II - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung
- III - To-Dos für die Übergangsfrist bis zur Geltung der DS-GVO

www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

Artikel 29 Datenschutzgruppe:

- WP243 Guidelines on Data Protection Officers ('DPOs')
- WP243 ANNEX – Frequently asked questions

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Vielen Dank für Ihre Aufmerksamkeit!