Datenschutzschulung

LSB
LANDESSPORTBUND THÜRINGEN
Mitten im Sport.

Thüringen, den 28.10.2017

BÜRO : MÜLOT

Zur Person

SACHVERSTÄNDIGENBÜRO MÜLOT

Name:	Dirk-Michael Mülot
Geburtsdatum / - Ort:	05. November 1959, Bielefeld
Staatsangehörigkeit:	Deutsch
Familienstand:	Verheiratet seit 1987, 2 Kinder
Schulausbildung:	Abitur
Berufsausbildung:	Informatiker (Wirtschaft)
Freier Sachverständiger (Fachbereiche):	Datenschutz, Datensicherheit, Forensische Informatik, Sicherheitskronometrie, Risikomanagement, Notfallplanung
Zertifizierungen:	TÜV zertifizierter Datenschutzbeauftragter, Datenschutzmanager und Datenschutzauditor, Cisco-Systems (CSE-SMB)
Berufliche Tätigkeiten:	Freier Sachverständiger, Senior-Berater, Externer Datenschutzbeauftragter, Datenschutzmanager, Auditor (Datenschutz & Datensicherheit), Fachreferent, Ausbilder und Prüfer für Datenschutzbeauftragte und -Auditoren
Spezialbereiche:	Datenschutz im Verein und Verband , Datenschutzmanagement in Konzernen, Unternehmensvorbereitung BSI-Audit (ISO 27000),

Zur Person

SACHVERSTÄNDIGENBÜRO MÜLOT

Aktivitäten im Sport	**Gelernter Pferdewirtschaftsmeister FN**
	Ehem. Kadermitglied der Vielseitigkeitsreiter
	Teilnehmer an internationalen Wettkämpfen
	Teilnehmer an Championaten
	Technischer Delegierter und Steward der FEI
	Parcourschef FN Springen und Gelände
	Richter der FN (Dessur, Springen, Vielseitigkeit)
	Co-Bundestrainer Para-Equestrian TEAM Germany 2007 bis 2014
	Honorartrainer Schweiz, Turkmenistan, Mexiko und Slowakei
	Vorsitzender eines Zucht-, Reit - und Fahrvereins (seit 15 Jahren), Aktiver Züchter

DS-GVO und BDSG-Neu

Herausforderung Datenschutz im Verein und Verband

DSGVO
(EU-Datenschutz-Grundverordnung)

Spannungsfeld zwischen Theorie und Praxis

Was ist Datenschutz

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Datenschutz ist:

1. Vielen nicht bekannt
2. Nervig und Lästig
3. Ein trockenes Thema
4. **Wichtig für jeden Einzelnen**
5. **Gesetzlich geregelt und ein Muss für**
   a. **jedes Unternehmen**
   b. **jeden Verein oder Verband**
   c. **jedes Projekt**
6. **Erfolgsfaktor!**

DSGVO - Ziel

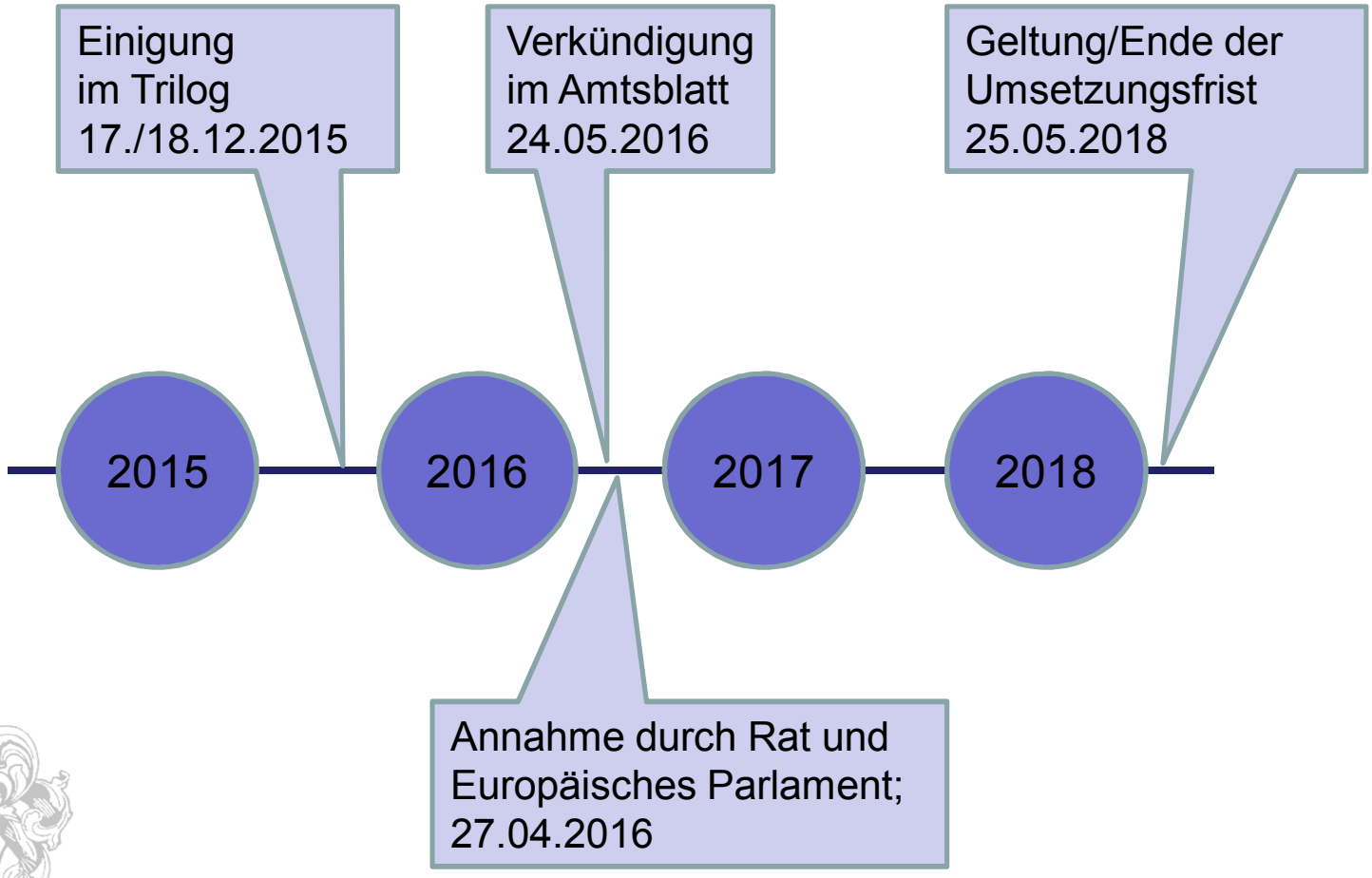
SACHVERSTÄNDIGENBÜRO MÜLOT

Es geht nicht darum, Daten zu schützen!

Es geht darum, den Betroffenen davor zu schützen, dass ihm durch die Erhebung, Verarbeitung und Nutzung seiner Daten ein Schaden entsteht!!!

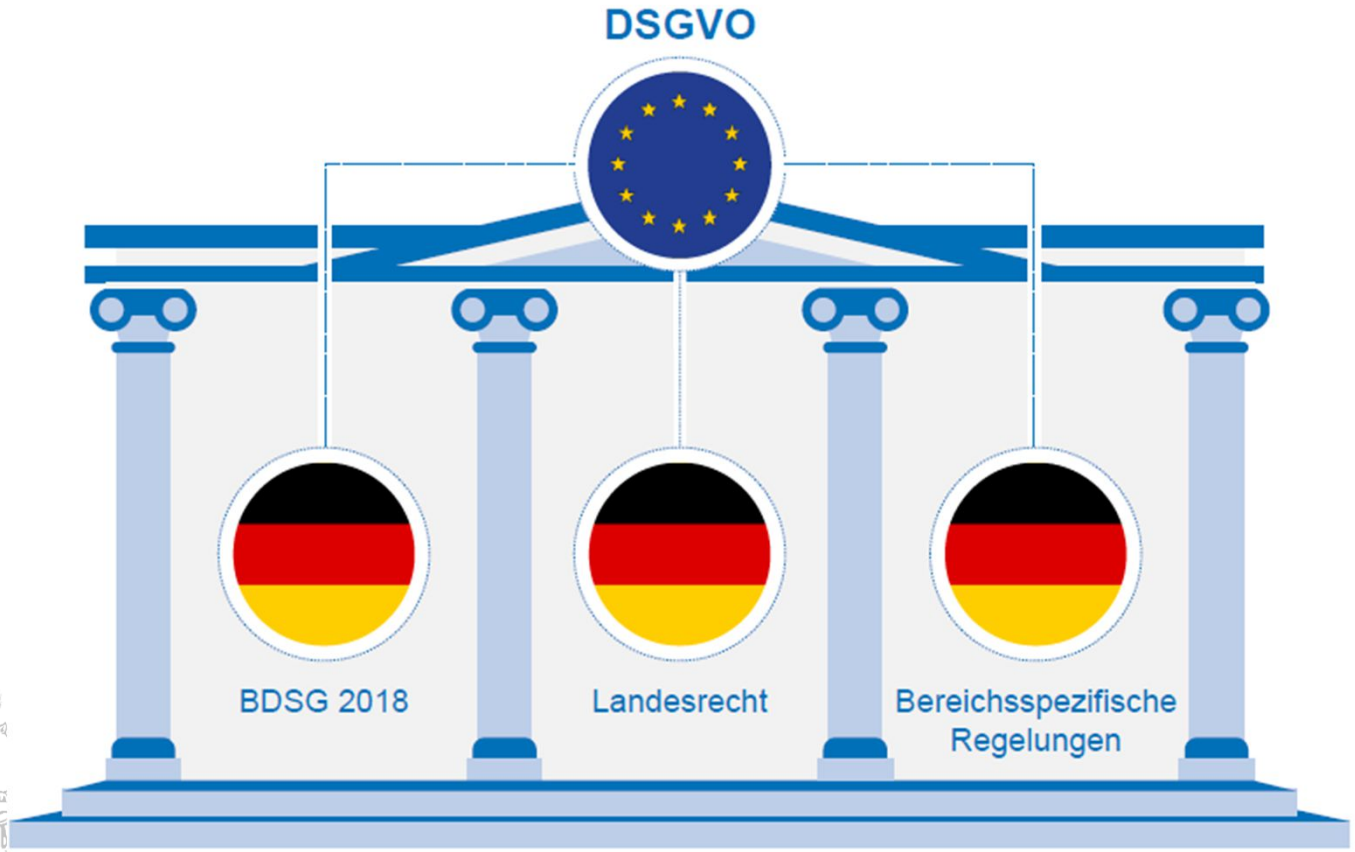
DSGVO: Timeline

SACHVERSTÄNDIGENBÜRO MÜLOT



BÜRO : MÜLOT

DSGVO: Deutsches Recht wird abgelöst



Die DSGVO…

SACHVERSTÄNDIGENBÜRO MÜLOT

… regelt das Recht auf Schutz persönlicher Daten als GRUNDRECHT innerhalb der EU

… vereinheitlicht weitgehend die derzeit bestehenden 28 nationalen Gesetze innerhalb der EU

… basiert auf den bestehenden datenschutzrechtlichen Bestimmungen.

… erhöht die Sanktionen bei Vergehen drastisch **(bis zu 20 Mio. € bzw. 4 % des weltweiten (Konzern-)Umsatzes)**

Die DSGVO…

SACHVERSTÄNDIGENBÜRO MÜLOT

… wird über die Aufsichtsbehörde sicherlich wesentlich strenger exekutiert als das BDSG bisher

… beinhaltet eine Meldepflicht (innerhalb von 72 Stunden an die Aufsichtsbehörde) und eine Beweislastumkehr

… setzt wesentlich mehr an Dokumentation voraus als das BDSG

… tritt mit 25. Mai 2018 EU-weit in Kraft

3 Säulen-Prinzip

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

DSGVO

Organisation

- Nominierung eines Datenschutzbeauftragten
- Richtlinien und Vorgehensweisen
- Aufbau eines DSMS

Prozesse

- Identifikation des relevanten Datenumfanges
- Einwilligung, Auskunft, Berichtigung, Löschung
- Datenschutzfolgeabschätzungen definieren und implementieren
- Training/Schulung

Systeme

- Überprüfung bezüglich Erfassung, Haltung, Verarbeitung und Speicherung von personenbezogenen Daten inkl. Anpassungen

Wichtige Begriffe

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Personenbezogene Daten	• Alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen, direkt oder indirekt über Name, Kennnummer, oder andere Merkmale (siehe Folgefolie)
Verantwortlicher	• Person oder Einrichtung, die personenbezogene Daten verarbeitet
Auftragsverarbeiter	• Person oder Einrichtung, die im Auftrag des eines Verantwortlichen personenbezogenen Daten verarbeitet
Dritte	• Personen oder Einrichtungen, die personenbezogene Daten verarbeiten dürfen, außer der betroffenen Person selbst, Verantwortliche oder Auftragsverarbeiter

Wichtige Begriffe

SACHVERSTÄNDIGENBÜRO MÜLOT

Betroffener

- Betroffene Person ist diejenige, deren Schutz das Gesetz zum Ziel hat und dem die Rechte aus dem Gesetz eingeräumt sind. Dabei handelt es sich um pbDaten einer bestimmten oder bestimmbaren natürlichen Person.

DSB – Datenschutz-Beauftragter

- Ein Datenschutzbeauftragter wirkt in einer Organisation auf die Einhaltung des Datenschutzes hin. Die Person kann Mitarbeiter dieser Organisation (bDSB) sein oder als externer Datenschutzbeauftragter bestellt werden.

Einwilligung

- Freiwillige und unmissverständlich abgegebene Erklärung oder sonstige eindeutige bestätigende Handlung, mit welcher die betreffende Person der Verarbeitung ihrer personenbezogener Daten zustimmt

Was sind personenbezogenen Daten?

SACHVERSTÄNDIGENBÜRO MÜLOT

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche** Person beziehen.
- Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung über persönliche oder sachliche Verhältnisse zum bspw.
  - Name, Vorname, Geburtsdatum, Alter, Familienstand,
  - Standortdaten (bspw. Anschrift),
  - Onlinekennung (bspw. Telefonnummer, E-Mail Adresse, IP-Adresse, usw.),
  - Kennnummer (bspw. Konto-, Kreditkartennummer, Kraftfahrzeugnummer, Kfz-Kennzeichen, Personalausweisnummer, Sozialversicherungsnummer,

Was sind personenbezogenen Daten?

SACHVERSTÄNDIGENBÜRO MÜLOT

- Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung über persönliche oder sachliche Verhältnisse zum bspw.
  - …
  - Wirtschaftliche, kulturelle oder soziale Identität,
  - Vorstrafen,
  - Werturteile (bspw. Zeugnisse, Kreditwürdigkeit)

  identifiziert werden kann.
- **Kundendaten** gehören ebenso zu den personenbezogenen Daten wie die **Personaldaten** von Beschäftigten

Besonders schützenswerte Daten

SACHVERSTÄNDIGENBÜRO MÜLOT

Die Verarbeitung personenbezogener Daten, aus denen die

- rassische und ethnische Herkunft,
- politische Gesinnung,
- religiöse oder weltanschauliche Überzeugungen, oder die
- Gewerkschaftszugehörigkeit

hervorgehen, sowie die Verarbeitung von

- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (auch Augenfarbe, etc.),
- Gesundheitsdaten (physische, physiologische, psychische Daten)

Besonders schützenswerte Daten

oder Daten zum

- Sexualleben oder der sexuellen Orientierung

einer natürlichen Person, ist grundsätzlich **untersagt** und bedarf einer **ausdrücklichen Einwilligung**.

Es gibt auch hier definierte Ausnahmen (z. B. Arbeitsrecht), d.h. die Verarbeitung ist **erforderlich**; auch gilt wenn die Verarbeitung zum **Schutz** lebenswichtiger Interessen der Person oder einer natürlichen Person erforderlich ist.

Wann dürfen personen-bezogene Daten verarbeitet werden?

SACHVERSTÄNDIGENBÜRO MÜLOT

- Wenn von der betroffenen Person eine **Einwilligung** zur Verarbeitung vorliegt.
  - Die Einwilligung muss zweifelsfrei nachgewiesen werden können
  - Zustimmung sowie Widerruf müssen in einfacher Sprache gleichermaßen präsent sein
  - Der Zweck der Verarbeitung muss in klaren Worten formuliert sein
  - Das Prinzip der Datenminimierung ist zu beachten
- Zur Abwicklung eines Vertrages
  - Es gilt ein Kopplungsverbot. An die Datenerhebung dürfen keine weiteren Angebote/Verträge gekoppelt werden.
- Zur Erfüllung rechtlicher Verpflichtungen
  - Rechtliche Aufbewahrungsfristen
  - Verträge
- Zur Wahrung öffentlicher Interessen

Grundsätze der DSGVO

SACHVERSTÄNDIGENBÜRO MÜLOT

- Personenbezogene Daten dürfen nur so lange **aufbewahrt** werden, wie es für den Zweck für den sie erhoben wurden, unbedingt erforderlich ist. Gesetzliche **Fristen** sind zu berücksichtigen
- **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** muss technisch und organisatorisch sichergestellt werden.
  DSGVO fordert auch die Belastbarkeit von Systemen und Dienste.
  Privacy by design (Technik) & default (Voreinstellungen).
- TOMs (**technische und organisatorische Maßnahmen**) müssen das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen, regelmäßig auf ihre Wirksamkeit hin überprüft, bewertet und evaluiert werden und den „Stand der Technik" umsetzen
- Der Verantwortliche ist für die **Einhaltung der Vorschriften** verantwortlich und muss diese **nachweisen** können.
  Auch wenn die Daten durch Dritte verarbeitet werden!!!
- DSGVO sieht nun datenschutzspezifische **Zertifizierungsverfahren** vor.
- Datenminimierung!

Grundsätze der DSGVO

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

- **Betroffenenrechte**
  - Informationspflicht bei Datenerhebung (Art. 13, Art. 14)
  - Auskunftsrecht inkl. Kopie der Daten (Art. 15)
  - Berichtigung, Korrekturbegehren (Art. 16)
  - Löschung, Löschungsbegehren (Art. 17)
  - Einschränkung (Art. 18)
  - Mitteilungspflicht bei Berichtigung, Löschung, Einschränkung der Verarbeitung (Art. 19)
  - Datenübertragbarkeit (Art. 20)
  - Widerspruch, Widerruf (Art. 21)
  - Profiling (Art. 22)

- **Alle Maßnahmen sollen unter Berücksichtigung der wirtschaftlichen Verhältnismäßigkeit getroffen werden**

Basisanforderungen für Vereine und Verbände

"Pflichtprogramm"

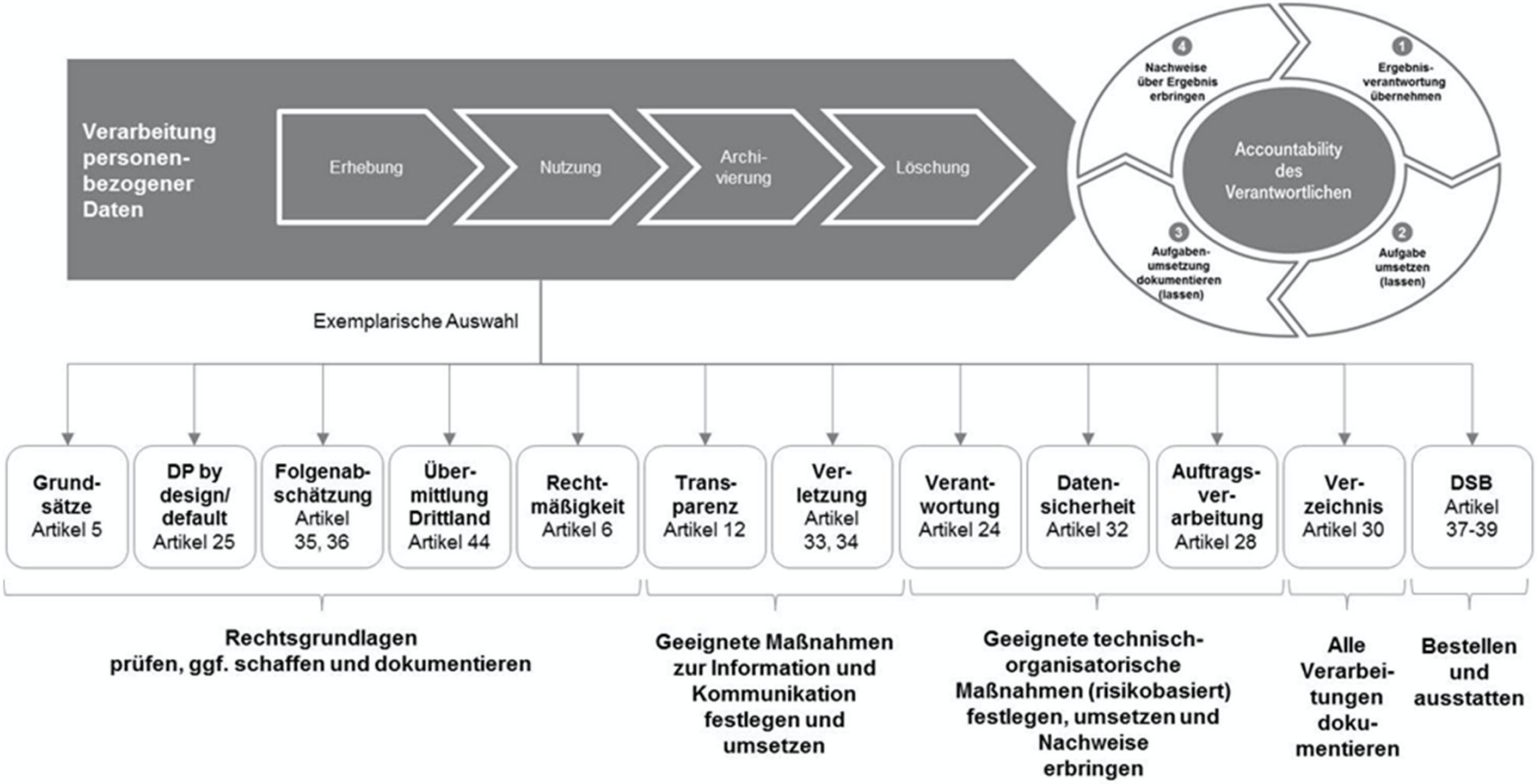
Aufgaben organisieren

Um die Anforderungen aus der Datenschutz-Grundverordnung (DSGVO) zu erfüllen, muss der Verantwortliche im Unternehmen einen bunten Blumenstrauß an Maßnahmen (risikobasiert) definieren, umsetzen, dokumentieren und kontrollieren – um dann festzustellen, dass die eigentliche Arbeit jetzt erst anfängt.

Denn die DSGVO baut im Ergebnis auf einem kontinuierlichen Verbesserungsprozess auf. Um dem gerecht zu werden, können sich die Aufgaben in einem P(lan)-D(o)-C(heck)-A(ct)-Zyklus organisieren lassen.

Aufgaben

SACHVERSTÄNDIGENBÜRO MÜLOT



Aufgaben des Verantwortlichen im PDCA-Zyklus dargestellt

Aufgaben

- Den Verantwortlichen, der personenbezogene Daten verarbeitet, treffen zahlreiche Pflichten aus der Grundverordnung.
- Entscheidend ist dabei zum einen, dass die Grundverordnung die umzusetzenden Anforderungen durch Nachweispflichten (Accountability) und hohe Bußgelder flankiert.
- Zum anderen geht die DSGVO offensichtlich davon aus, dass es nicht damit getan ist, einmalig ein Datenschutz-Management-System im Unternehmen einzurichten. Vielmehr betont sie die Notwendigkeit, das System an die konkreten Umstände anzupassen.
- Damit hängen die Maßnahmen, die Unternehmen ergreifen müssen, letztlich von dynamischen Faktoren ab. Das betrifft in erster Linie die konkrete Bedrohungslage im unternehmensindividuellen Kontext gemäß aktuellem Stand der Technik.

Aufgaben

Veränderung ist normal

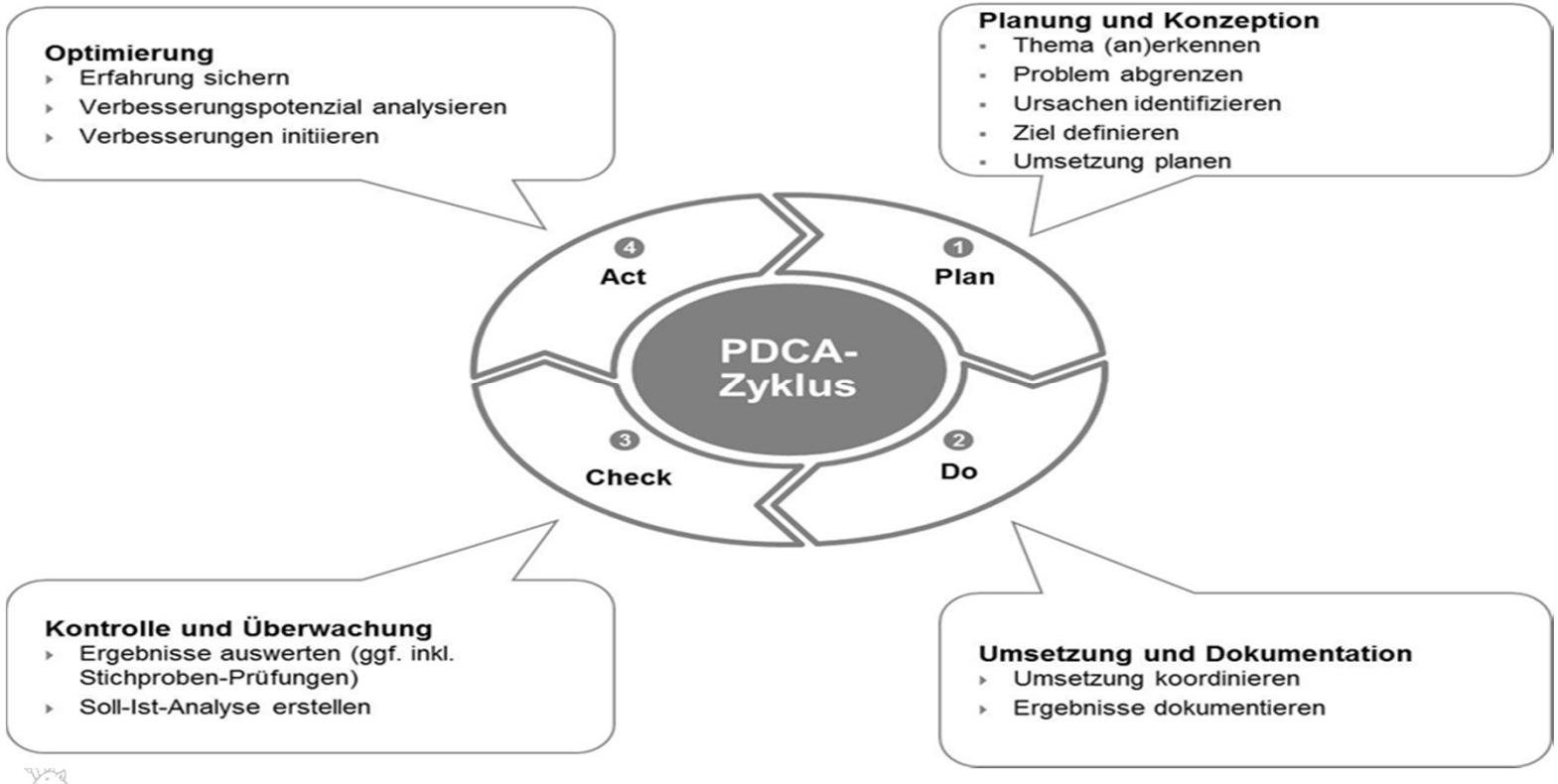
- Nicht nur in der IT-Welt ist Veränderung mittlerweile der Normalzustand. In Zeiten der digitalen Transformation kann sich kaum ein Unternehmen der ständigen Anpassung entziehen.
- Das bedeutet in der unternehmerischen Konsequenz: Bestimmte Aufgaben sind eigentlich nie erledigt, sondern als wiederkehrender Zyklus zu wiederholen. Nur so lässt sich feststellen, ob das Unternehmen den selbst gestellten bzw. vorgegebenen Anforderungen genügt (oder ob es zu viel investiert).
- Statt sich über die Veränderung zu ärgern, wird sie zur Quelle der ständigen Optimierung.

Der PDCA-Zyklus

- Die unternehmerische Wiederholungsschleife aus „Plan" (Planung), „Do" (Umsetzung), „Check" (Kontrolle) und „Act" (Optimierung), kurz PDCA-Zyklus, beschreibt einen kontinuierlichen Verbesserungsprozess.
- Der PDCA-Zyklus ist die Antwort auf eine sich ändernde Umgebung (Markt, Wettbewerb, Bedrohungslage, rechtliche Rahmenbedingungen etc.).
- Im Einzelnen zählen dazu die folgenden Phasen/Schritte:
  - Plan – Planung und Konzeption
  - Do – Umsetzung und Dokumentation
  - Check – Kontrolle und Überwachung
  - Act – Optimierung

Der PDCA-Zyklus

SACHVERSTÄNDIGENBÜRO MÜLOT

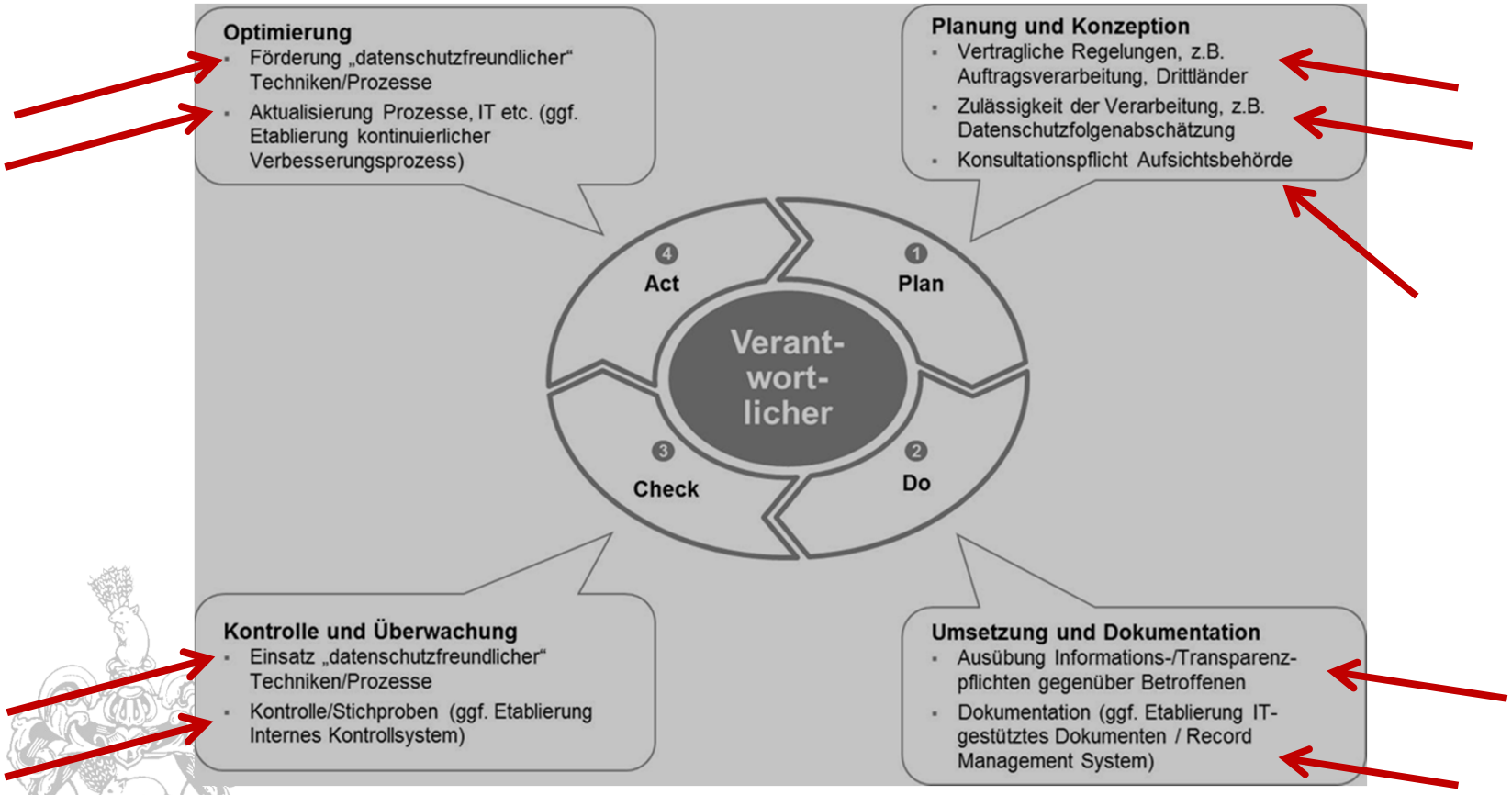


- Im Idealfall ist das beim PDCA-Zyklus jederzeit der Fall. Denn der Zyklus sieht von vornherein die (wiederkehrende) Planung vor. Der Zyklus ist gerade darauf ausgelegt, auf Veränderungen zu reagieren.

DSGVO-Anforderungen PDCA-Zyklus

SACHVERSTÄNDIGENBÜRO MÜLOT

Über den Lebenszyklus von personenbezogenen Daten im Unternehmen hinweg stellt die DSGVO hohe Anforderungen an die zulässige und ordnungsgemäße Verarbeitung.



DSGVO-Anforderungen
PDCA-Zyklus

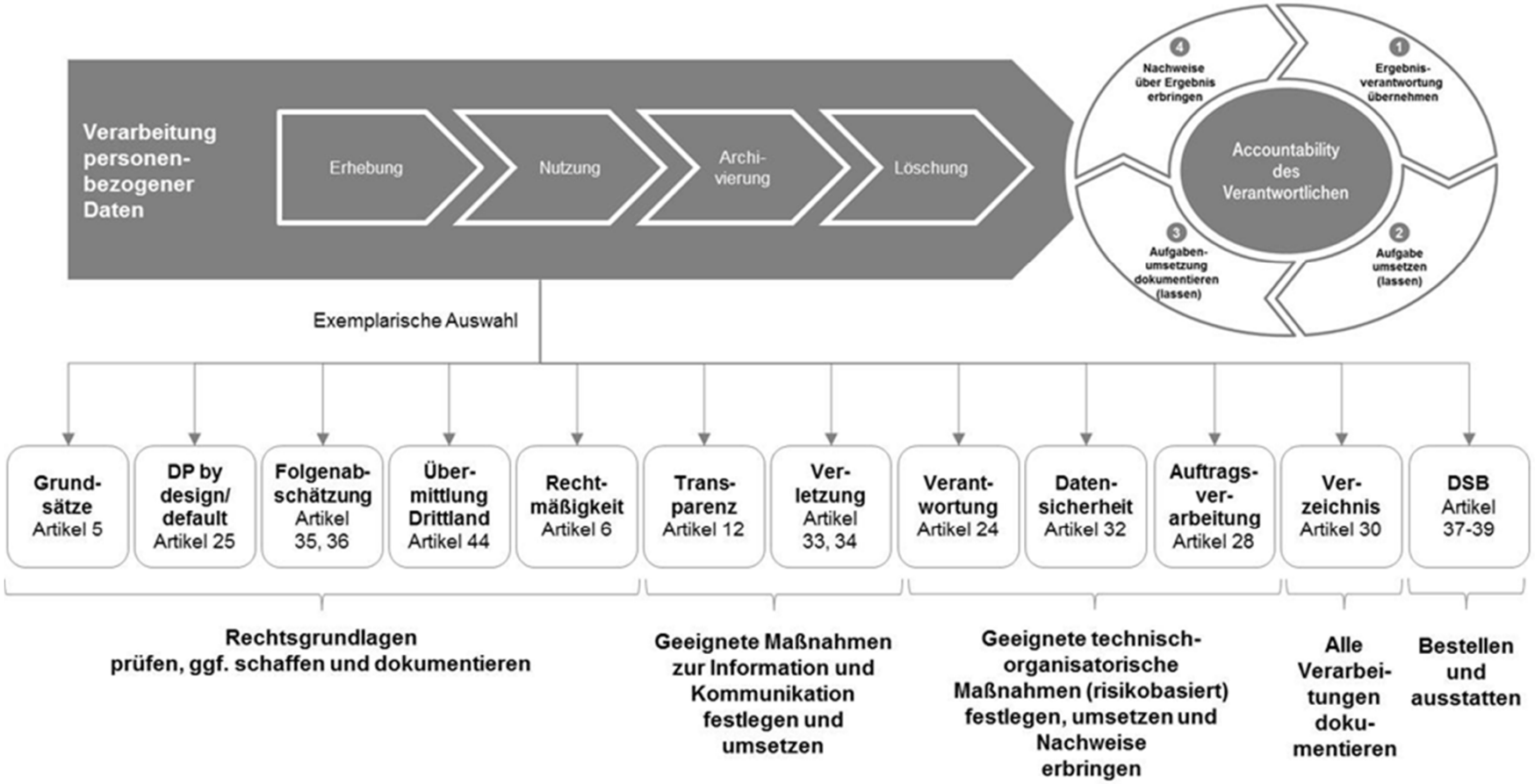
Damit der Verantwortliche die an ihn gestellten Anforderungen nachweisbar und aktuell erfüllen kann, kommt im Idealfall ein Datenschutz-Management-System (DSMS) zum Einsatz. Es fördert datenschutzfreundliche Techniken und Voreinstellungen und muss stets weiterentwickelt werden.

Im Kern basiert jedes moderne Management-System auf einem kontinuierlichen Verbesserungsprozess. Es ist darauf ausgerichtet, ein Thema und in der Folge spezifische Anforderungen im Unternehmen zu etablieren.

DSGVO-Anforderungen PDCA-Zyklus

SACHVERSTÄNDIGENBÜRO MÜLOT

Die Grundlage dafür kann der PDCA-Zyklus sein. Die Aufgaben aus der Grundverordnung lassen sich exemplarisch wie in der folgenden Abbildung gezeigt eingruppieren:



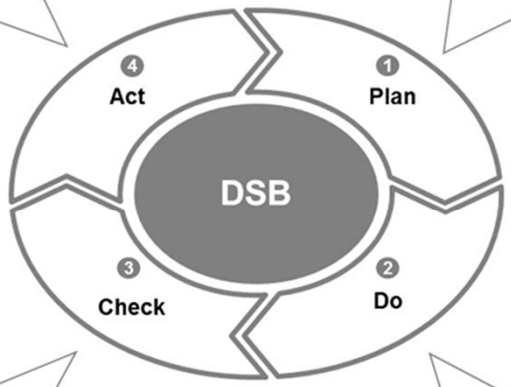
DSGVO-Anforderungen PDCA-Zyklus

SACHVERSTÄNDIGENBÜRO MÜLOT

In gleicher Weise lassen sich auch die Aufgaben des Datenschutzbeauftragten im Sinne der Beratung und Überwachung exemplarisch wie folgt dem PDCA-Zyklus zuordnen:

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

Planung und Konzeption
- Beratung, z.B. bei der Erstellung von Unternehmensrichtlinien (Policies)
- Überwachung, z.B. bei Anfragen im Rahmen der Datenschutzfolgen-abschätzung



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

Umsetzung und Dokumentation
- Grundsätzlich nicht in Tagesgeschäft (der Fachbereiche) involviert
- Ggf. Unterstützung im Einzelfall

FAZIT

- Die DSGVO ist vor dem Hintergrund deutlich gestiegener Bußgelder nicht nur angesichts der Fülle ihrer (gerade auch dokumentatorischen) Anforderungen eine Herausforderung für Unternehmen. Auch die Ausrichtung und Orientierung an Strukturelementen aus anderen Management-Disziplinen wie dem IT-Sicherheits- und Risikomanagement führt dazu, dass sich die Einrichtungen bei der Herangehensweise stärker an äußeren Gegebenheiten und Standards werden orientieren müssen.

- Nicht nur auf wirtschaftlicher Ebene wird der Wettlauf um die kontinuierliche Verbesserung ausgetragen. Er steckt – angesichts stetig neuer IT-Bedrohungen – eben auch und gerade in der zulässigen und ordnungsgemäßen Verarbeitung von personenbezogenen Daten.

FAZIT

- Um dieses Ziel zu erreichen, bietet sich ein Ansatz an, der sich bei Herangehensweise und Organisation am PDCA-Zyklus orientiert, um die immer wieder zu kontrollierenden DSGVO-Aufgaben in den Griff zu bekommen. Insofern stellt der PDCA-Zyklus sozusagen den Kern eines jeden Datenschutz-Management-Systems dar.

Datenschutzorganisation- Basisanforderungen an Aufbau- und Ablauforganisation

Wesentliche Datenschutzvorschriften der DS-GVO(1)

Die Grundanforderungen an den Verantwortlichen sind zunächst in Art. 5 Abs. 2 und Art. 24 Abs. 1 geregelt. Art. 5 Abs. 2 bestimmt, dass der **Verantwortliche für die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten verantwortlich** ist und dies nachweisen können muss („Rechenschaftspflicht"). Damit ist die Einhaltung der in Art. 5 Abs. 1 geregelten materiell-rechtlichen Vorgaben gemeint, also die folgenden Grundsätze:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
- **Zweckbindung**
- **Datenminimierung**
- **Richtigkeit der Daten**
- **Speicherbegrenzung**
- **Integrität und Vertraulichkeit**

Wesentliche Datenschutzvorschriften der DS-GVO (2)

Art. 24 Abs. 1 formuliert die **Pflichten des Verantwortlichen im Hinblick auf die zu ergreifenden technischen und organisatorischen Maßnahmen**. Erforderlich sind Maßnahmen, um „sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt". Diese Maßnahmen sind erforderlichenfalls zu überprüfen und zu aktualisieren.

Vorschriften DS-GVO

- Von diesem Grundverständnis ausgehend sind die wesentlichen Umsetzungserfordernisse für Unternehmen, Vereine und Verbände in den Art. 12 bis 23 (Rechte der Betroffenen) und in den Art. 24 bis 43 (Verantwortlicher und Auftragsverarbeiter) geregelt. Dies zeigt anschaulich die nachfolgende Übersicht:

Vorschriften DS-GVO

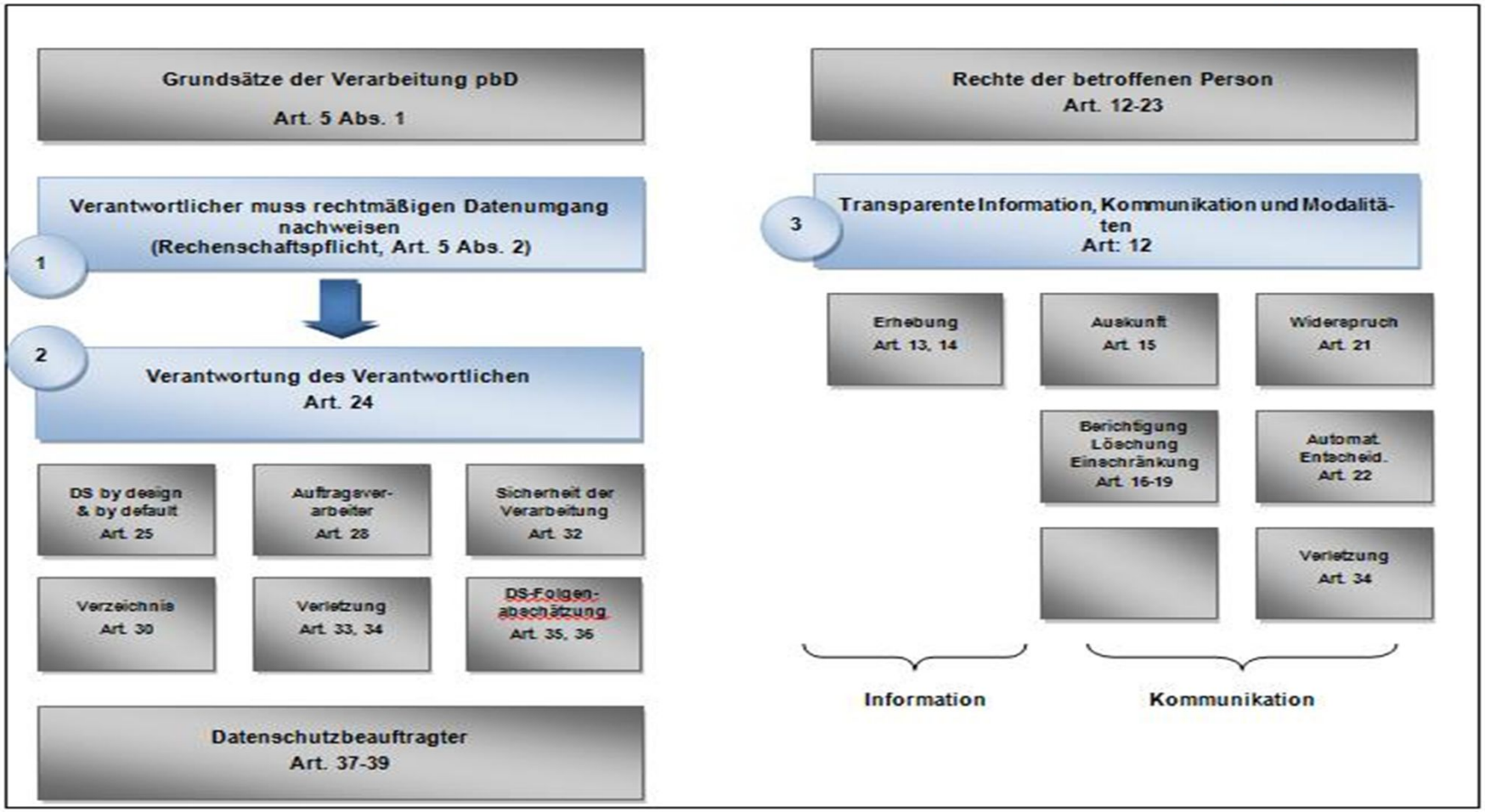


Abbildung 1: Wesentliche Datenschutzvorschriften
Hinzu kommen noch die Vorschriften, die bei einer Übermittlung in ein Drittland (also ein Nicht-EU-bzw. EWR-Mitgliedsland) berücksichtigt werden müssen (Art. 44-49).

Wesentliche Datenschutzprozesse (Ablauforganisation)

DEFINITION „Prozesse“:

Unter einem Prozess wird eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Aktivitäten) verstanden, die ausgeführt werden, um ein bestimmtes Ziel zu erreichen, z. B.

- Gewährleistung der datenschutzkonformen Verarbeitung,
- Sicherstellung der Betroffenenrechte oder der
- datenschutzgerechten Handhabung von Datenschutzverletzungen.

Er wird durch ein definiertes Ereignis ausgelöst, z. B. neu geplante Datenverarbeitung, Auskunftsersuchen eines Betroffenen oder im Fall einer Datenschutzverletzung.

Ein Verfahren hingegen ist ein geregelter, in einzelne Schritte zerlegbarer, nachvollziehbarer und wiederholbarer Ablauf.

Wesentliche Datenschutzprozesse (Ablauforganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Die Umsetzung des Datenschutzes kann aus Unternehmenssicht in drei Kernprozesse unterteilt werden:

1. Datenschutzkonforme Datenverarbeitung
2. Sicherstellung der Betroffenenrechte
3. Handhabung von Datenschutzverletzungen

Wesentliche Datenschutzprozesse (Ablauforganisation)

Im Einzelnen zu den drei Kernprozessen

Im Zentrum jeder datenschutzrechtlichen Betrachtung steht zunächst die Verarbeitung der personenbezogenen Daten. Diese muss rechtlich zulässig sein. Dementsprechend betrachtet diese Handlungshilfe den Prozess **„Datenschutzkonforme Verarbeitung"** als einen der drei Kernprozesse.

- Risikobeurteilung,
- Datenschutz-Folgenabschätzung und
- Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen

sind bspw. Unterprozesse zu diesem Kernprozess.

Wesentliche Datenschutzprozesse (Ablauforganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Daneben steht der Kernprozess der Umsetzung der Betroffenenrechte (z. B. Recht auf Auskunft). Auch dieser Prozess ist in den Unternehmensalltag zu integrieren. Im Fokus der Betrachtung steht dabei der Betroffene. Wir nennen diesen Prozess nachfolgend **„Sicherstellung der Betroffenenrechte".**

Wesentliche Datenschutzprozesse (Ablauforganisation)

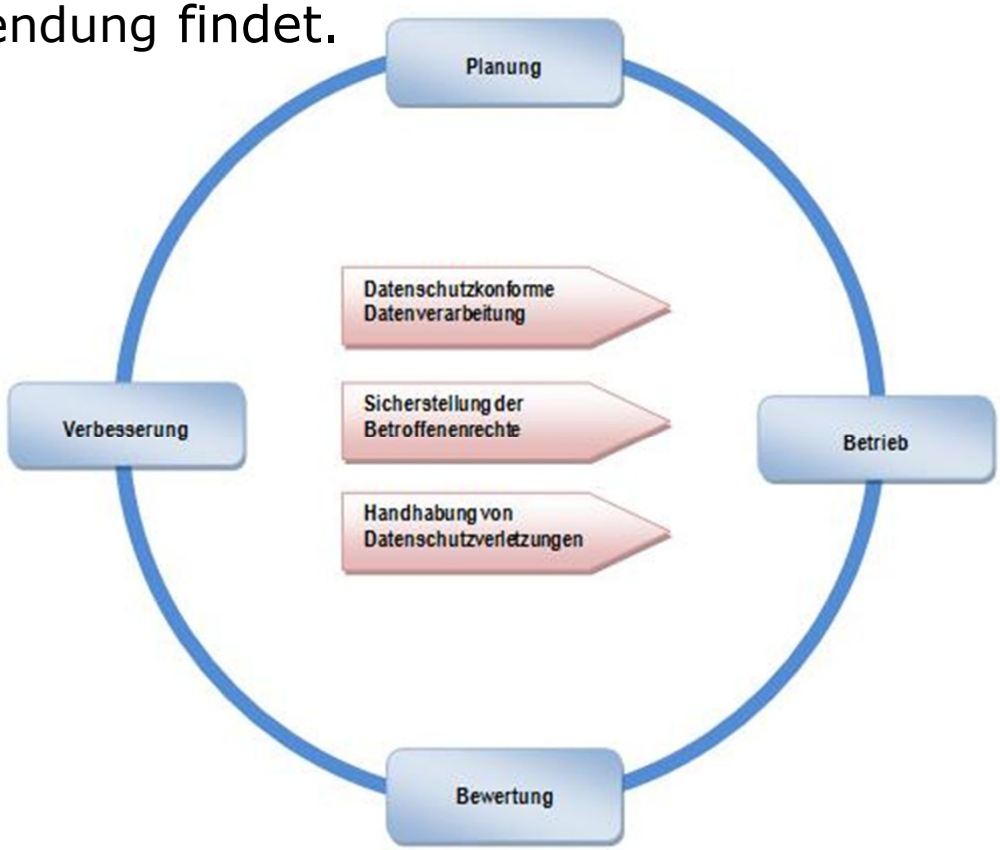
Schließlich ist ein dritter Kernprozess zur Einhaltung der datenschutzrechtlichen Bestimmungen erforderlich, nämlich das Vorgehen bei sog. **„Datenschutzverletzungen".**

- Gemeint ist die gesetzlich in Art. 4 Nr. 12 definierte „Verletzung des Schutzes personenbezogener Daten", welche gem. den Art. 33 bis 34 Melde- und Benachrichtigungspflichten auslösen kann. Eine Verletzung liegt vor, wenn die Sicherheit der Daten verletzt wurde und dies zu einer Vernichtung, einem Verlust, zur Veränderung oder zur unbefugten Offenlegung der oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat. Die prozess-orientierte Umsetzung dieser Vorgaben ist besonders plastisch: Nur, wenn das Unternehmen Vorkehrungen getroffen hat, die sicherstellen, dass eine Datenschutzverletzung rechtzeitig bemerkt, adressiert und gemeldet wird, ist eine Einhaltung der Vorgaben in den Art. 33 bis 34 möglich.

Wesentliche Datenschutzprozesse (Ablauforganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT

Die nachfolgende Grafik zeigt, das für alle drei Kernprozesse das **PDCA-Modell** mit den Phasen Planung, Betrieb, Bewertung und Verbesserung Anwendung findet.



Wesentliche Datenschutzstrukturen (Aufbauorganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT

Neben den Datenschutzprozessen, die die Abläufe regeln, bedarf es bestimmter organisatorischer Strukturen, um die Einhaltung der Datenschutzanforderungen sicherzustellen. Die wesentlichen Elemente, die die Aufbauorganisation festlegt sind:

- **Datenschutzziele**
- **Datenschutz-Governance-Struktur sowie**
- **Datenschutzleitlinie**

Wesentliche Datenschutzstrukturen (Aufbauorganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Im Einzelnen zu den drei Hauptelementen;

Die Datenschutzziele leiten sich aus dem Sinngehalt der Datenschutzgesetze ab und dienen zur Steuerung des Datenschutzes im Unternehmen. Die Datenschutzziele müssen durch die Geschäftsleitung als Unternehmensziele bestimmt werden. Sie sind wiederum ein wesentlicher Bestandteil der Datenschutzleitlinie.

Wesentliche Datenschutzstrukturen (Aufbauorganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Die Datenschutz-Governance-Struktur ist ein Steuerungsansatz für den Datenschutz und definiert Rollen und Verantwortlichkeiten in Abhängigkeit von den organisatorischen Rahmenbedingungen.

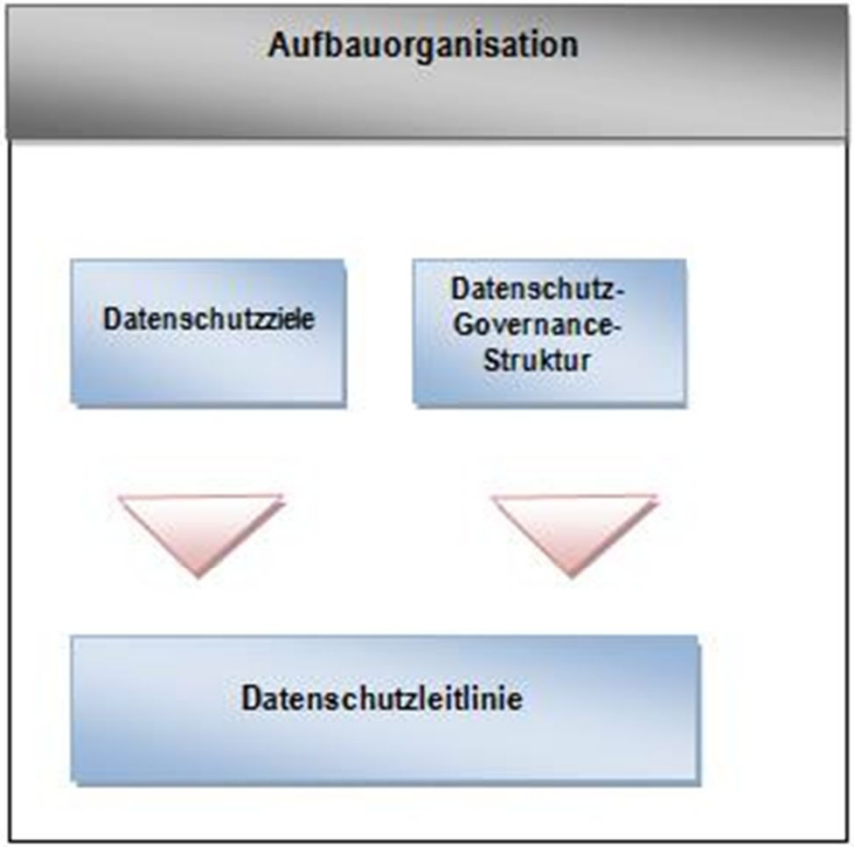
Wesentliche Datenschutzstrukturen (Aufbauorganisation)

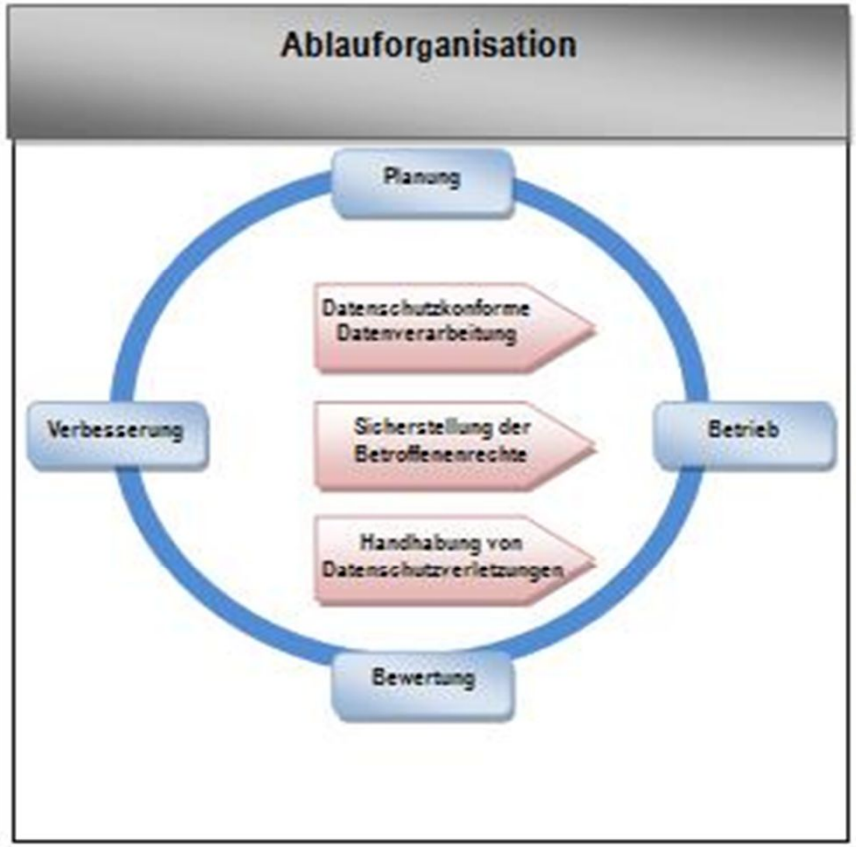
SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

Die Datenschutzleitlinie ist eine Selbstverpflichtung des Unternehmens, in der sich das Unternehmen selbst gewählte Datenschutzziele auferlegt. Sie enthält die Governance-Struktur zur Zuweisung der Verantwortlichkeiten und wird von der Geschäfts-leitung verabschiedet. Die nachfolgende Übersicht zeigt den Zusammenhang der Aufbau- und Ablauforganisation auf.

Wesentliche Datenschutzstrukturen (Aufbauorganisation)

SACHVERSTÄNDIGENBÜRO MÜLOT





Datenschutzaufbau- und -ablauforganisation

FAZIT
DATENSCHUTZMANAGEMENT

SACHVERSTÄNDIGENBÜRO MÜLOT

Die Datenschutz-Grundverordnung stellt sowohl Für die Unternehmen als auch für die Aufsichtsbehörden einen Paradigmenwechsel dar.

Aus Sicht der Unternehmen -„Verantwortungsvolles Datenschutz-Management"

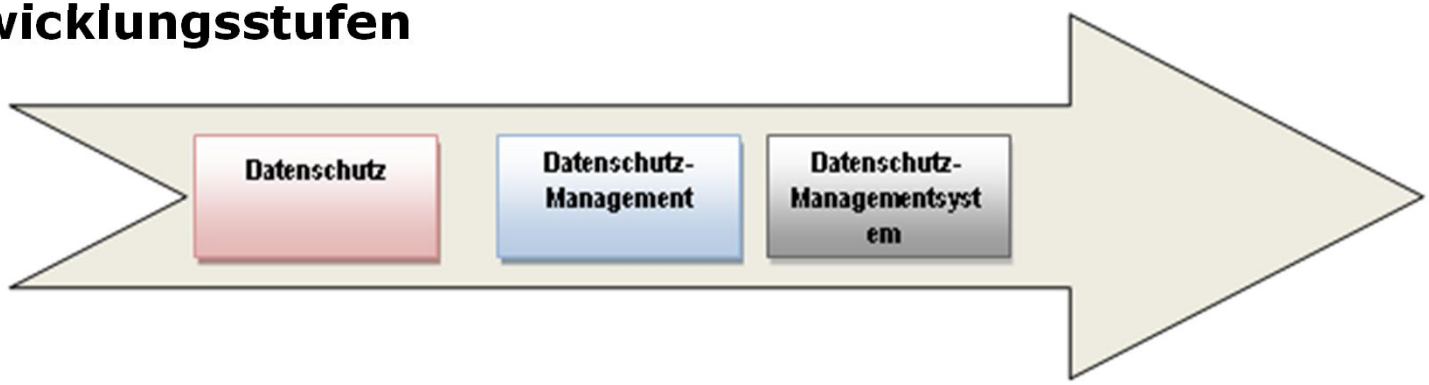
Die umfangreichen Anforderungen und Pflichten der DS-GVO an die Unternehmen (Verantwortlicher und Auftragsverarbeiter), insbesondere die Rechenschaftspflicht, führen zu einem Paradigmenwechsel. Konformität mit der Verordnung und Erfüllung der Rechenschaftspflichten sind nur durch ein angemessenes Datenschutz-Management zu erreichen. Ein angemessenes Datenschutz-Management kann nur durch ein vollumfängliches proaktives Managementsystem realisiert werden.

FAZIT
DATENSCHUTZMANAGEMENT

SACHVERSTÄNDIGENBÜRO MÜLOT

Der Datenschutz erfordert ein effektives Compliance Management-System, das dadurch geprägt ist, dass es proaktiv, transparent, formell, vollumfänglich, prozessorientiert, risikobasiert und integriert ist.

Entwicklungsstufen



Entwicklung des Datenschutzes hin zu einem effektiven Compliance-Management-System

Schritte zur Erfüllung der „Rechenschaftspflicht"

Datenschutz ist originäre Aufgabe des Vorstandes / der Geschäftsführung, wie sich auch aus Art. 5 Abs. 2 DS-GVO ergibt:

Der „Verantwortliche" also ist verantwortlich für die Erhaltung der Datenschutzgrundsätze. Diese Einhaltung ist nachzuweisen („Rechenschaftspflicht").

FAZIT
DATENSCHUTZMANAGEMENT

SACHVERSTÄNDIGENBÜRO MÜLOT

Schritte zur Erfüllung der „Rechenschaftspflicht"

Die nachfolgenden 12 Schritte zeigen die wesentlichen Themen, mit denen sich die Unternehmen, insbesondere der Vorstand / die Geschäftsführung, nunmehr beschäftigen müssen:

- **Compliance mit der EU-DS-GVO ist „Chefsache"**
- **Interdisziplinäres Team zusammenstellen**
- **Sich mit der Datenschutz-Grundverordnung vertraut machen**
- **Bestandsaufnahme**
- **Überarbeitung des Verzeichnisses der Verarbeitungstätigkeiten**
- **Überprüfung der Rechtsgrundlagen für die Verarbeitung**
- **Überprüfung der Informations- und Mitteilungspflichten**
- **Überprüfung der technischen und organisatorischen Maßnahmen**
- **Überprüfung der Auftragsverarbeitung**
- **Überprüfung der Übermittlung in Drittländer**
- **Datenschutz prozessorientiert und risikobasiert betrachten**
- **die zuständige Aufsichtbehörde konsultieren**

Datenschutzorganisation
- Als Basisbestandteil der Rechenschaftspflicht

Übersicht der wichtigsten Dokumente

SACHVERSTÄNDIGENBÜRO MÜLOT

Konzept und DSMS

Datenschutz-Unternehmens-Richtlinie und Ziele	Verarbeitungs-Verzeichnis, VV-Verwaltung	Schutzbedarf und Risikoniveau/-klasse Risikobehandlungsmethodik und -plan
Gesetzliche, behördliche und vertragliche Anforderungen	DSFA, DSFA-Verwaltung	Schaden- und Schadensklasse für den Betroffenen und das Unternehmen
Verhaltensregeln (akzeptable Nutzung von pbDaten), Codes-of-Conduct	Betroffenenrecht Anfragen, Betroffenenrecht Verwaltung	Richtlinie Übergreifende Schutzmaßnahmen (Technische- und organisatorische Maßnahmen)
DS-Organisationsstruktur, DSMS	Verwaltung der DS-Vorfälle/Verletzungen	Sicherheits-Rollen und Verantwortlich-keiten (Rollen- und Rechtekonzept)
Bestellung Datenschutz-Beauftragter und Meldung an die Aufsichtsbehörde	Meldung Aufsichtsbehörde	Kryptokonzept, Anonymisierungskonzept
Verzeichnis der Services und der Verarbeitungen von pbDaten	Auftragsverarbeiter-Richtlinien, -Vertrag und -Verwaltung	Notfallkonzept
	Incident DS-Management-Verfahren, Vorgehensweise bei Betroffenenrechte	Schulung zu Datenschutz

Ein weiteres Kernthema „Datensicherheit“

Definitionen

Datenschutz = (WAS?)

Alle rechtlichen Vorgaben zum Umgang mit Informationen (Daten) insbesondere den personenbezogenen Daten.

Datensicherheit = (WIE?)

Alle technischen- und organisatorischen Maßnahmen, welche die Vorgaben des Datenschutzes sicherstellen.

Wahrung der Persönlichkeitsrechte

SACHVERSTÄNDIGENBÜRO MÜLOT

Durch Sicherstellung der…..

- **Vertraulichkeit (Schutz vor unberechtigtem Zutritt, Zugang, Zugriff)**

  z.B. Berechtigungssysteme, Prozessmodellierung (Vergabe und Entzug von Rechten)
- **Integrität (Schutz vor Manipulation / Veränderung)**

  z.B. Zugriffsberechtigungssysteme – Explizitrechte, Datensicherung
- **Verfügbarkeit (Schutz vor Verlust oder Zerstörung)**

  z.B. Datensicherung / Systemsicherung, Systemschutz / Ausfallsysteme / Wiederanlaufkonzepte

Wahrung der Persönlichkeitsrechte

…. sowie Garantie der …..

- **Authentizität (Nachvollziehbarkeit der Quelle und des Verfassers)**

  Sicherstellung, dass Daten tatsächlich vom Verfasser stammen und nicht gefälscht /verändert wurden.

- **Revisionsfähigkeit (Prüfbarkeit)**

  Die Beteiligung an einer datenbezogenen Aktion/Transaktion darf nicht zu leugnen sein.

- **Transparenz (Dokumentation)**

  Die einzelnen Verfahren und Aktionen/Transaktionen sind vollständig, aktuell und nachvollziehbar zu dokumentieren.

Art. 32 DSGVO
Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

Sicherheit

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Sicherheit

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Sicherheit

- Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Sicherheit

- Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Erwägungsgrund 78

Geeignete technische und organisatorische Maßnahmen

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. …

Erwägungsgrund 78

Geeignete technische und organisatorische Maßnahmen

…

Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. …

Erwägungsgrund 78

Geeignete technische und organisatorische Maßnahmen

… In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

Technikregelungen der Datenschutzgesetze

SACHVERSTÄNDIGENBÜRO MÜLOT

„Kontrollarten"

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle

- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- zweckbezogene Verarbeitung

„technikoffene Schutzziele" *

- Verfügbarkeit
- Integrität
- Vertraulichkeit

- Transparenz
- Authentizität
- Revisionsfähigkeit
- Nichtverkettbarkeit
- Intervenierbarkeit

- Systemdatenschutz
- Audit / Zertifizierung
- Selbstdatenschutz

** Eckpunkte der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert" (18.3.2010)*

Zudem TOM nach § 64 BDSG-NEU

SACHVERSTÄNDIGENBÜRO MÜLOT
Sicherheitskronometrie : Forensische Informatik : Datenschutz : Datensicherheit : Risk-Management :

- Zutrittskontrolle / Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit der Systeme
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

Was ist zu tun- 1?

SACHVERSTÄNDIGENBÜRO MÜLOT

- Bestellung eines DSB und Meldung an das LDI
- Festschreibung von Wertigkeit und Stellenwert Datenschutz (GF/V)
- Ggf. Aufnahme der Datenschutzziele in der Satzung
- Schulung der im Umgang mit pbD beauftragten Personen
- Erstellen der Verarbeitungsübersicht (Liste)
- Datenschutz prozessorientiert und risikobasiert betrachten
- Prüfung der Verarbeitungsübersicht bzgl. Beschreibungspflicht
- Durchführung von Datenschutz-Folgenabschätzungen (DSFA)

Was ist zu tun- 2?

SACHVERSTÄNDIGENBÜRO MÜLOT

- Aufbau der notwendigen Prozesse zur Sicherstellung der Betroffenenrechte
- Prozesse einführen zur Überprüfung der Rechtsgrundlagen für die Verarbeitung
- Prozesse einführen zur Überprüfung und Sicherstellung der Informations- und Mitteilungspflichten
- Ausrichtung der Datensicherheit an die gesetzlichen Vorgaben
- Prüfung der Auftragsverarbeitungen und Anpassung der Verträge
- Meldeprozess an die zuständige Aufsichtbehörde etablieren
- Auslandsdatenverarbeitung / - Übermittlung prüfen
- Prüfung der Einwilligungserklärungen ggf. Anpassung
- Aufbau und Einführung eines prüffähigen (DSMS)

Fazit Datenschutz/DSGVO

SACHVERSTÄNDIGENBÜRO MÜLOT

- ✓ Datenschutz ist Chefsache
- ✓ Es wird kompliziert: „**Ein Gesetz geht, zwei Gesetze kommen**"
- ✓ Erhebliche Veränderungen gegenüber der bisherigen Rechtslage: **Betroffenenrechte werden gestärkt, Unternehmenspflichten ausgebaut**
- ✓ **Bußgeldrahmen steigt drastisch: bis zu 4% des globalen Vorjahresumsatzes**;
  Fast jede Vorschrift der DSGVO ist bußgeldbewehrt
- ✓ Es geht nicht mehr ohne: **Effektive Datenschutz-Management-Systeme sind gefragt**
- ✓ Neue Möglichkeiten der datenschutz-rechtlichen Compliance: **Datenschutz-Zertifizierung als Chance**
- ✓ Datenschutz ist ein **Erfolgsfaktor**

Datenschutz kann man nicht kaufen

Datenschutz muss man schaffen

BÜRO : MÜLOT

Fragen ???

SACHVERSTÄNDIGENBÜRO MÜLOT

Was sollten wir jetzt noch klären?