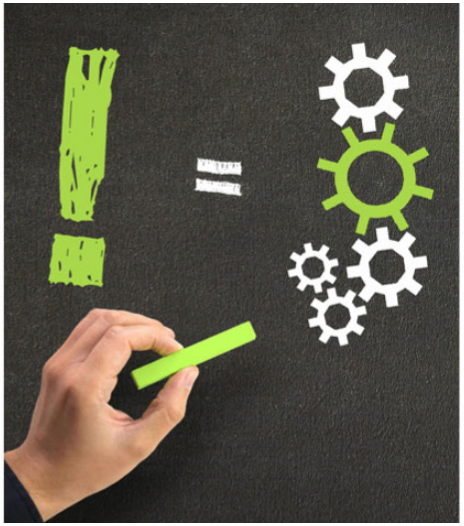



Die neue EU-Datenschutzgrundverordnung

DSGVO

Warum Datenschutz-Grundverordnung?

Unabweisbarer Reformbedarf:

- Geltendes EU-Recht von 1995
- Heterogene Gesetzgebung in den 28 Mitgliedsstaaten
- Heterogene Aufsicht und Durchsetzung innerhalb der EU

Warum Datenschutz-Grundverordnung?
Unabweisbarer Reformbedarf

- Weitgehende Vollharmonisierung wurde **nicht** erreicht
  - Unbefriedigende Antworten auf Globalisierung
- Anwendungsbereich sehr weitgehend auf in EU niedergelassene Unternehmen beschränkt
- Nicht mehr an die aktuellen technologischen Entwicklungen angepasst

Warum Datenschutz-Grundverordnung?

Lösungen?

- Stärkere Harmonisierung durch Rechtsform der Grundverordnung
- Unmittelbar anwendbares Recht
- Einheitliche Regeln im Binnenmarkt auch für Nicht-EU-Unternehmen
- Marktortprinzip
- Vereinheitlichte Durchsetzung des Datenschutzrechts
- Maßvolle Modernisierung

Warum Datenschutz-Grundverordnung?

Lösungen?

Datenschutzgrundverordnung

Aufbau der DSGVO

Systematischer Aufbau folgt weitgehend der RL 95/46/EG

DSGVO enthält 11 Kapitel:

- Kapitel I:
  Allgemeine Bestimmungen
  - Anwendungsbereich,
  - Begriffsbestimmungen
- Kapitel II:
  Grundsätze Prinzipien, Zulässigkeit, besonders sensible Daten
- Kapitel III:
  Rechte der betroffenen Person Informationsrechte, Recht auf Vergessen, Datenportabilität, Profiling

Aufbau der DSGVO

Systematischer Aufbau folgt weitgehend der RL 95/46/EG

DSGVO enthält 11 Kapitel:

- Kapitel IV: Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
  - Techn./organisatorische Pflichten,
  - Auftragsverarbeiter,
  - Meldung von DS-Verstößen,
  - DPIA „Data Protection Impact Assessment“,
  - bDSB,
  - Code of Conduct,
  - Zertifizierung

Aufbau der DSGVO

Systematischer Aufbau folgt weitgehend der RL 95/46/EG

DSGVO enthält 11 Kapitel:

- Kapitel V:

  Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisatıonen

- Kapitel VI: Unabhängige Aufsichtsbehörden
  - Unabhängigkeit, Rechtsstellung, Aufgaben, Befugnisse
- Kapitel VII: Zusammenarbeit und Kohärenz
  - Kooperation der Aufsichtsbehörden in Europa, Europäischer Datenschutzausschuss

Aufbau der DSGVO

Systematischer Aufbau folgt weitgehend der RL 95/46/EG

DSGVO enthält 11 Kapitel:

- Kapitel VIII:
  Rechtsbehelfe, Haftung und Sanktionen
  - Beschwerde- und Klagemöglichkeiten, Schadensersatz, Bußgelder
- Kapitel IX:
  Vorschriften für besondere Verarbeitungssituationen
  - Medienprivileg, Beschäftigtendatenschutz, Forschung, Religionsgemeinschaften
- Kapitel X:
  Delegierte Rechtsakte und Durchführungsrechtsakte
- Kapitel XI:
  Schlussbestimmungen
  - u. a. Verhältnis zur ePrivacy-RL

Die DSGVO Grundsätze

Die EU DSGVO

…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 Grundsätze

…wird über die Aufsichtsbehörde wesentlich strenger exekutiert als das BDSG

…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

DSGVO
Wesentliche Inhalte

- DSGVO unterscheidet systematisch nicht zwischen öffentlichem und nicht-öffentlichem Bereich
  - Fortschreibung der RL 95/46/EG
  - Wesentlicher Unterschied zu DEU

- Grundsätzlich keine Rücksicht auf föderales System
  - Ausnahme: Vertretung im EDSA (Europäischer Datenschutzausschuss)

DSGVO
Wesentliche Inhalte

- DSGVO enthält allgemeine Regelungen, viele unbestimmte Rechtsbegriffe

  - Datenschutz-**GRUND**verordnung!
  - Erheblicher Konkretisierungsbedarf durch:
    - Öffnungen für Mitgliedsstaaten-Recht
    - Aufsichtsbehörden/EDSA (Europäischer Datenschutzausschuss)
    - Delegierte Rechtsakte, Durchführungsrechtsakte

Bewährte Prinzipien

Verfassungsrechtliche Prinzipien geben den Rahmen vor:

- Art. 7 der EU-Grundrechtecharta
  - Achtung des Privat- und Familienlebens
- Art. 8 der EU-Grundrechtecharta
  - Datenschutzgrundrecht
- Art. 16 AEUV (Vertrag über die Arbeitsweise der europäischen Union)
  - Gesetzgebungsauftrag an Rat und EP
- Grundsteine für zentrale Architektur in Tradition BVerfG

Bewährte Prinzipien

Verfassungsrechtliche Prinzipien geben den Rahmen vor:

- Ist Autonomie noch zeitgemäß?
  - Gewaltmonopol des Staates, Überwachungsstaat?
  - Monopolisierung im Bereich der Datenverarbeitung durch die Wirtschaft
  - Alternativlosigkeit bei der Inanspruchnahme von Dienstleistungen
  - Kommerzialisierung der Daten -> „Daten als Währung des 21. Jahrhunderts“

- Recht auf informationelle Selbstbestimmung -> Autonome Entscheidung des Einzelnen als Legitimation für DV

- Darüber hinaus Verbot jeder Verarbeitung personenbezogener Daten, sofern nicht gesetzlich zugelassen

Bewährte Prinzipien

Verfassungsrechtliche Prinzipien geben den Rahmen vor:

- Viel Kritik durch Wirtschaft und Wissenschaft
- Wie frei ist man wirklich?
- Wieviel Selbstbestimmung ist möglich?
- Grundrechte und Primärrecht lassen keinen Spielraum für andere Konzeptionen zum Schutz der Privatsphäre
- EuGH hat bewährte Prinzipien gestärkt!

Bewährte Prinzipien

Weitere wichtige Prinzipien:

- Erforderlichkeit/Angemessenheit/Datensparsamkeit
  - Beschränkung auf das jeweils notwendige Maß
  - Widerspruch zu Big Data?
- Zweckbindung
  - Wie weit lassen wir Weiterverarbeitung zu anderen Zwecken zu?
- Transparenz
  - Auskunfts-, Informations-, Berichtigungs-,Löschungsansprüche

Bewährte Prinzipien

Weitere wichtige Prinzipien:

- Datensicherheit
  - Datenschutzfreundliche Technologien, Privacy by Design/Default
- Angemessenes Datenschutzniveau beim Datenexport
- Unabhängige Aufsicht
- Effektive Durchsetzung

Neue Akzente

Im Überblick….

Marktortprinzip	Profiling	Internationaler Datentransfer
Vollharmonisierung (öffentlichen Bereich)	Stärkere Betonung des TOM Datenschutzes	One-Stop-Shop
Betroffenenrechte	Stärkung der Selbstregulierung	Rechtsdurchsetzung

Neue Akzente
Im einzelnen….

- Marktortprinzip
  - Art. 3(2): DSGVO gilt auch für Verantwortliche ohne Niederlassung in der EU, wenn sie auf dem EU-Markt tätig sind

- Vollharmonisierung grundsätzlich auch im öffentlichen Bereich
  - Ausnahme Polizei und Justiz ->JI-Richtlinie (EU-Richtlinie für Justiz und Inneres: Datenschutz oder Überwachung)

- Erweiterung der Betroffenenrechte
  - Erweiterte Informationspflichten
  - „Recht auf Vergessen“, Datenportabilität,
  - Erweiterte Widerspruchsrechte

Neue Akzente
Im einzelnen….

- Profiling

- Stärkere Betonung des technischen und organisatorischen Datenschutzes
  - Privacy by Design/Privacy by Default
  - Zum Teil Anerkennung von Gewährleistungszielen der Datensicherheit
  - Meldung über Datenschutzverletzungen (Data Breach Notification)
  - Datenschutzfolgeabschätzung
  - Betriebliche/Behördliche Datenschutzbeauftragte

Neue Akzente
Im einzelnen….

- Stärkung der Selbstregulierung
  - Verhaltensregeln (Codes of Conduct)
    - z. B. für Verbände / Firmenzusammenschlüsse
  - Audit und Zertifizierung
    - durch Bundesländer, Bundesbeauftragte, auf europäischer Ebene, TÜV?, Zulassung durch Datenschutzbehörden
- Modernisierung beim Internationalen Datentransfer
  - Stärkere Betonung unternehmensinterner Regulierung
  - Sektorielle Anerkennung eines angemessenen DS-Niveaus
  - Regeln für Übermittlung an ausl. Behörden und Gerichte

Neue Akzente
Im einzelnen....

- Kooperation der Aufsichtsbehörden (One-Stop-Shop)
  - Schaffung verbindlicher Kooperationsmechanismen
  - Verbindliche Entscheidungen durch EDSA (Europäischer Datenschutzausschuss)

- Wirksame Rechtsdurchsetzung
  - Besserer Rechtsschutz für Betroffene
  - Deutlich höhere Bußgelder (20 Mio €, 4% des weltweiten Umsatzes)

Föderales System und Datenschutz-Grundverordnung
Deutschland im europäischen Verbund

- Föderale Aufsichtsstruktur in Deutschland bleibt unverändert
- Deutsche Aufsichtsbehörden müssen im Europäischen Kontext mit einer Stimme sprechen
  - Höherer Abstimmungsaufwand
  - Stärkerer Einigungsdruck
- Europäische Kooperationsmechanismen müssen in Deutschland abgebildet werden

EUROPÄISCHE ENTSCHEIDUNGS-MECHANISMEN

One-Stop-Shop
Was ist das...?

- Instrument zur verbindlichen Entscheidung von Einzelfällen durch die Aufsichtsbehörden bei grenzüberschreitender Verarbeitung
  - Nicht im öffentlichen Bereich
  - Auf Einigung ausgerichtete Kooperation der Aufsichtsbehörden
  - Notfalls verbindliche Entscheidung durch EDSA

- Grenzüberschreitende Verarbeitung i. S. v. Art. 4(23):
  - Verarbeitung in mehreren Mitgliedsstaaten bei mehreren Niederlassungen in verschiedenen Mitgliedsstaaten oder
  - erhebliche Auswirkungen auf Betroffene in mehr als einem Mitgliedsstaat

Vorteile One-Stop

Für die Unternehmen:

- Federführende Behörde als zentraler Ansprechpartner am Sitz der Haupt-niederlassung
- Durchsetzung europaweit verbindlicher Entscheidungen
- Lokale Fälle bleiben lokal

Für die Betroffenen:

- Beschwerdemöglichkeit vor Ort
- Bescheidung der Beschwerden vor Ort
- Rechtsschutz vor Ort

One-Stop-Shop
Und die Aufsichtsbehörden?

- Sorgen durch komplexe Abstimmungsmechanismen für den reibungslosen Ablauf des One Stops
- Führen europaweit verbindliche Entscheidungen herbei
- Tragen so zur Konkretisierung und zugleich Harmonisierung des europäischen Datenschutzrechts bei

One-Stop-Shop
Funktionsweise

- Grundidee:
  Zuständigkeitskonzentration bei der Aufsichtsbehörde am Sitz der Hauptniederlassung (oder einzigen Niederlassung) -> Federführende Behörde

- Hauptniederlassung, Art. 4(16)
  - Ort der Hauptverwaltung, sofern die Entscheidungen über Zwecke und Mittel der DV nicht in anderer NL getroffen werden

- Alle anderen Behörden können betroffene Behörden sein, wenn
  - im Hoheitsgebiet ihres Mitgliedstaaten eine (weitere) NL besteht
  - eine Verarbeitung erhebliche Auswirkungen auf Betroffene im Mitgliedstaat hat
  - bei ihnen eine Beschwerde eingereicht wurde

One-Stop-Shop
Ergebnis

- Entweder Einigung aller beteiligten Aufsichtsbehörde (federführende und betroffene Behörden) mit der Folge der Verbindlichkeit für alle beteiligten Aufsichtsbehörden, Art. 60(6)

- Oder verbindliche Streitbeilegung im EDSA nach Art. 65
  - Entscheidung durch den EDSA innerhalb eines Monats nach Befassung mit 2/3-Mehrheit
  - Begründete Verlängerungsoption von einem weiteren Monat
  - Verstreicht zweite Frist, dann innerhalb weiterer 2 Wochen Entscheidung mit einfacher Mehrheit
  - Entscheidung erfolgt jeweils durch einzelne Aufsichtsbehörde

Fälle für Kohärenzverfahren

Kohärenzverfahren:

- Verpflichtung zur Zusammenarbeit und einheitlichen Rechtsanwendung für die Aufsichtsbehörden untereinander und mit der Kommission zusammenzuarbeiten

Fälle für Kohärenzverfahren

- EDSA* gibt in weiteren Fällen Stellungnahmen ab, Art. 64 (1):
  - Liste der Datenschutz-Folgenabschätzungen
  - Vereinbarkeit von Code of Conduct (CoC) mit DSGVO
  - Akkreditierungskriterien von Überwachungsstellen bei CoC und Zertifizierungsstellen
  - Festlegung von Standardklauseln und Genehmigung von Vertragsklauseln bei Drittstaatentransfer
  - Genehmigung von BCR (Binding Corporate Rules)

** EDSA = Europäische Datenschutz Aufsicht*

Fälle für Kohärenzverfahren

- Nach Art. 64(2) Stellungnahme zu Angelegenheiten allgemeiner Bedeutung in mehr als einem Mitgliedstaaten

  - Jede Aufsichtsbehörde,
  - der EDSA-Vorsitz und
  - die EU-Kommission

  sind antragsberechtigt

Weiteres Verfahren bei Stellungnahme EDSA

- EDSA entscheidet binnen acht Wochen mit einfacher Mehrheit, Art. 64(3)
- Nach Art. 64(7) trägt Aufsichtsbehörde dem Beschluss weitgehend Rechnung
- Folgt die Aufsichtsbehörde dem Beschluss nicht, erfolgt die verbindliche Streitbeilegung durch den EDSA nach Art. 65

Datenschutzgrundverordnung
DSGVO

- Siehe in der Anlage eine Übersicht der Änderungen zwischen BDSG und DSGVO:

- Starke Betonung der Sicherheit der personenbezogenen Daten – Sicht des Betroffenen!

- Grundsätzliche Schutzziele:
  - Verfügbarkeit,
  - Integrität,
  - Vertraulichkeit

Wichtige Stichpunkte:

Datenschutzfolgeabschätzung:

- Für Verarbeitungen von pbD, die eine hohes Risiko für die Rechte der Betroffenen darstellen können(!) muss ein eigene Risikoabschätzung erfolgen.

Datenschutzfolgeabschätzung DSFA

Für Unternehmen , z. B. Technologiehersteller, Systemintegratoren, IT-Diensteanbieter (Zugang, Inhalte etc.)

- Es ist offensichtlich, dass es einen Interessenkonflikt gibt, wenn die Organisation, die die DSFA durchführt, gleichzeitig ein gewichtiges Risiko für den Datenschutz darstellt.
- Um auszuschließen, dass sich die Organisation in den blinden Fleck der Risikoanalysen setzt, sollte wenigstens eine nachträgliche Überprüfung durchgeführt werden.
- Auch vom internen Datenschutzbeauftragten ist zu erwarten, dass er die Betroffenenperspektive einnimmt und seine eigene Organisation „von außen" betrachtet.
- Idealerweise sollte die DSFA aber von einer unabhängigen Instanz (jedoch in enger Kooperation mit der den Prüfgegenstand betreibenden Organisation) durchgeführt werden.

Datenschutzfolgeabschätzung DSFA

- Hier bleibt abzuwarten welche Vorschläge zur Umsetzung durch den „Arbeitskreis Technik“ der Landes- und der Bundesbeauftragten gemacht werden.

- Sind die Vorschläge die in der Anlage des „Forums Privatheit“ gemacht werden für alle Unternehmen (KMU-Unternehmen)?

Datenschutzgrundverordnung
DSGVO

Weitere Themen:

Veränderung im Bereich Auftragsdatenverarbeitung (Artikel 24, 28):

- ALT:
  Auftraggeber ist alleine für die Verarbeitung beim Dienstleister verantwortlich (Verfahren, TOM´s, Regelungen, etc.)

- NEU:
  Auch der Auftragnehmer muss die Verfahren betrachten und ist mitverantwortlich für die Verarbeitungen!

Privacy by Design

Privacy by Design – Ganzheitlicher Ansatz

Angemessene technische & organisatorische Maßnahmen

Ziel: Datenschutz freundliche Systeme

ENISA – Stand der Technik

Link

Privacy by Design

- Privacy by Design verfolgt einen auch aus anderen Standards und rechtlich- regulatorischen Regelwerken bekannten ganzheitlichen Ansatz des risikoorientierten Wirkzusammenhangs.

- Gemäß Artikel 23 DSGVO sollen angemessene technische und organisatorische Maßnahmen, datenschutzfördernde Technologien und datenschutzfreundliche Voreinstellungen in Zukunft von Anfang an integraler Bestandteil im Designprozess zur Entwicklung datenschutzfreundlicher Systeme und Dienstleistungen zur Verarbeitung personenbezogener Daten werden.

- Im Bericht "Privacy and Data Protection by Design - from policy to engineering" stellt die ENISA (Europäische Agentur für Netz- und Informationssicherheit) grundsätzlich dar, was als Stand der Technik gelten sollte, und erläutert, dass datenschutz- und sicherheitsunterstützende Vorgehensweisen und Techniken in der Entwicklung von der Praxis bislang vernachlässigt wurden.

Recht auf Vergessen

Recht auf Vergessen

Anspruch auf Lösung der
Personenbezogenen Daten

Recht auf Vergessen

- Eine betroffene Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein "Recht auf Vergessenwerden", wenn die Speicherung ihrer Daten gegen diese Verordnung oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt.

- Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn die personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt.

Licht und Schatten?

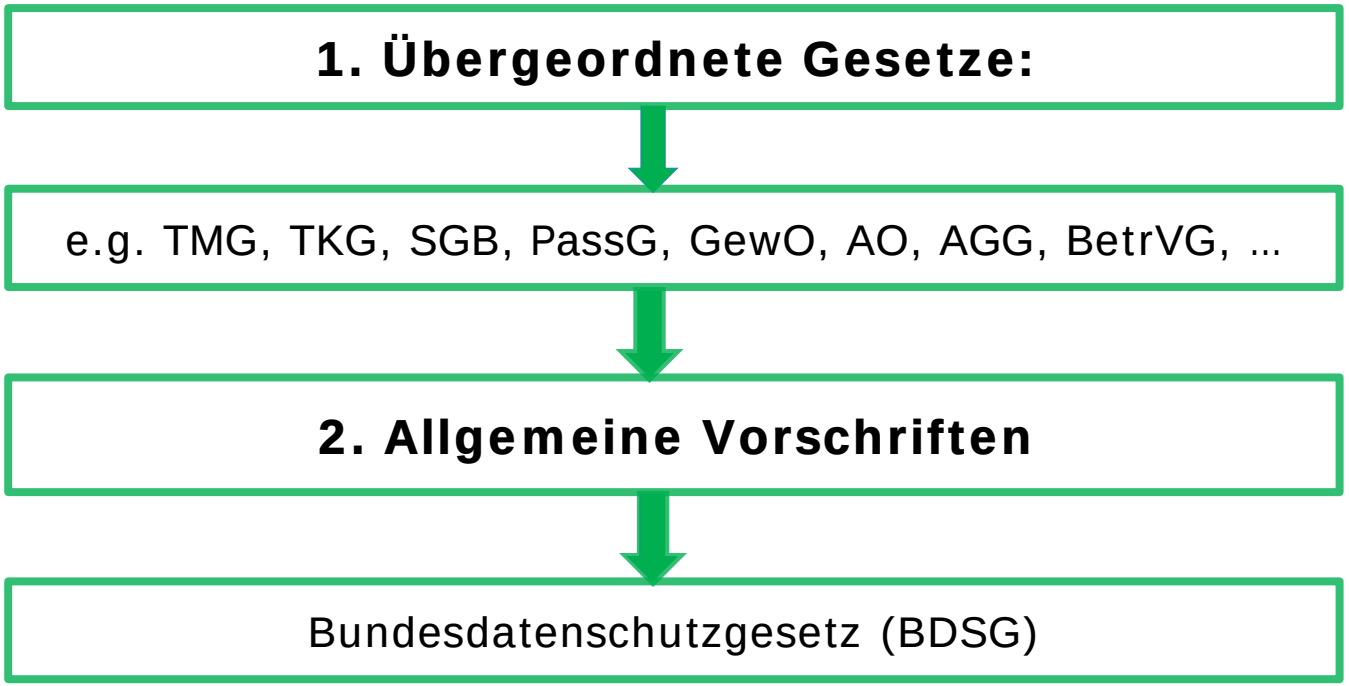
- Hohe Bußgelder drohen
  - Können existentiell für Unternehmen werden
  - Es bleibt abzuwarten wie die Aufsichtsbehörden hier vorgehen.
  - Weiterhin attraktiv bleiben große Firmen, da hier Bußgelder eine große Öffentlichkeitswirkung entfalten
- Durch Öffnungsklauseln für die Mitgliedsstaaten wird der ursprüngliche Sinn der DSGVO, eine Vereinheitlichung des europäischen Datenschutzrechts zu erreichen verwässert.
- Beispiele:
  - Der deutsche Datenschutzbeauftragte wird wahrscheinlich aus dem BDSG gem §4f genauso übernommen.
  - Ebenso der §32 BDSG Beschäftigtendatenschutz

Licht und Schatten?

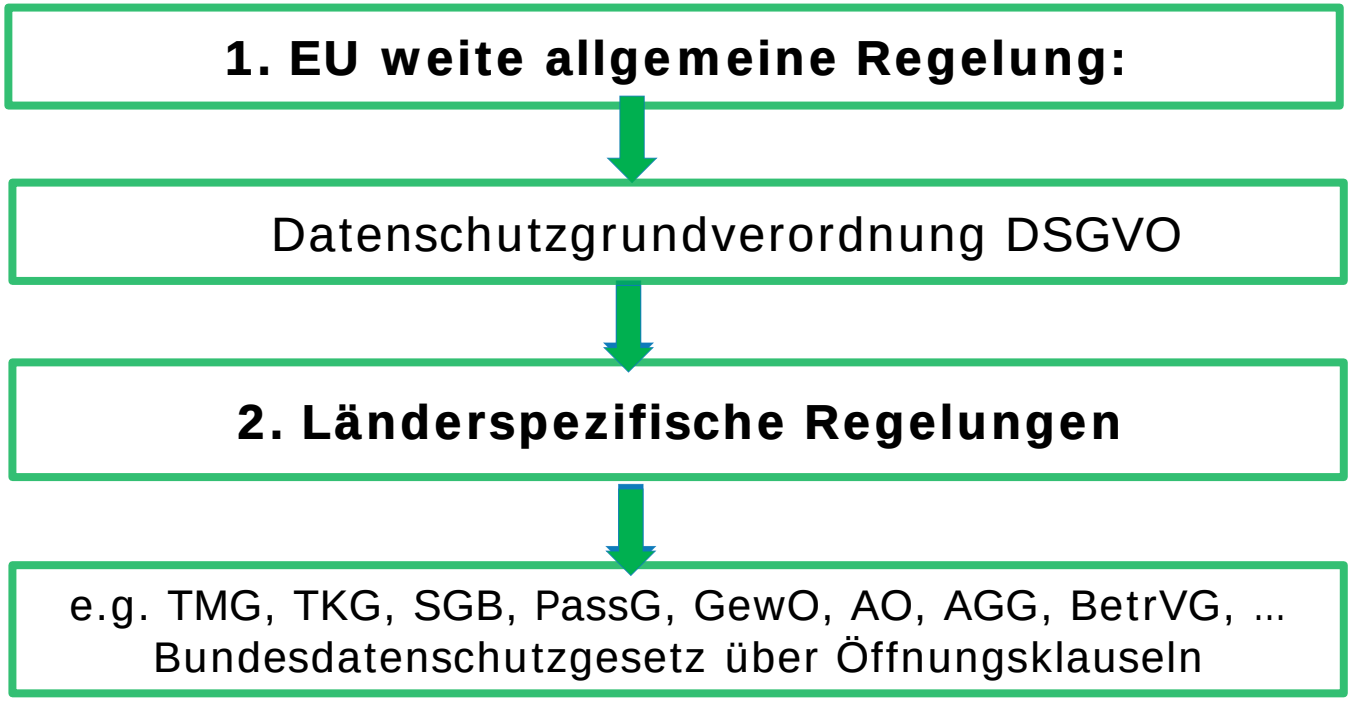
- Neuausrichtung des Datenschutzes in den Unternehmen: Alles auf Anfang!?

- Herausforderung der Unternehmen durch starke Betonung der IT-Sicherheit aus Sicht des Betroffenen.

Derzeitige Rechtslage in Deutschland



Zukünftige rechtliche Situation



Anonymisierung
BDSG vs DS Grundverordnung

§3 (6) BDSG

- Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

DSGVO

- Nicht definiert, aber die Prinzipien des Datenschutzes können nicht auf anonymisierte Daten angewendet werden

Pseudonymisieren
BDSG vs DS Grundverordnung

§3 (6a) BDSG

- Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Artikel 4 (5) DSGVO

- „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

Profiling
BDSG vs DS Grundverordnung

BDSG

- Nicht definiert

Artikel 4 (5) DSGVO

- „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

Grundsätze BDSG

§3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

§4 Zulässigkeit der Datenerhebung,-verarbeitung und –nutzung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Grundsätze DSGVO (Artikel 5)

Personenbezogene Daten müssen:

Rechtmässig

Zweckbindung

Datenminimierung

Grundsätze DSGVO (Artikel 5)

Personenbezogene Daten müssen:

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; („Zweckbindung“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

Grundsätze DSGVO (Artikel 5)

Personenbezogene Daten müssen:

Richtigkeit

Speicherbegrenzung (Dauer)

Integrität und Vertraulichkeit

Grundsätze DSGVO (Artikel 5)

Personenbezogene Daten müssen:

- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; („Speicherbegrenzung“)
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtig-tem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schä-digung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Grundsätze DSGVO (Artikel 6)

Rechtmäßigkeit

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: :

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

Grundsätze DSGVO (Artikel 6)

Rechtmäßigkeit

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: :

- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Grundsätze DSGVO (Artikel 7) Einwilligung

- Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

- Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

Grundsätze DSGVO (Artikel 7) Einwilligung

- Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Grundsätze DSGVO (Artikel 9)

Besondere pbD

Die Verarbeitung personenbezogener Daten, aus denen die

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder
- weltanschauliche Überzeugungen oder die
- Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von
- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder Daten zum
- Sexualleben oder der
- sexuellen Orientierung einer natürlichen Person ist untersagt.

Grundsätze DSGVO (Artikel 9)

Besondere pbD

dies gilt nicht in folgenden Fällen: :

- Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedsstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
- die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann,[...]
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

Weitere Rechte

Artikel 13: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Artikel 15: Auskunftsrecht der betroffenen Person

Artikel 16: Recht auf Berichtigung

Artikel 17: Recht auf Löschung („Recht auf Vergessenwerden“)

Artikel 18: Recht auf Einschränkung der Verarbeitung

Artikel 19: Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Artikel 20: Recht auf Datenübertragbarkeit

Artikel 21: Widerspruchsrecht

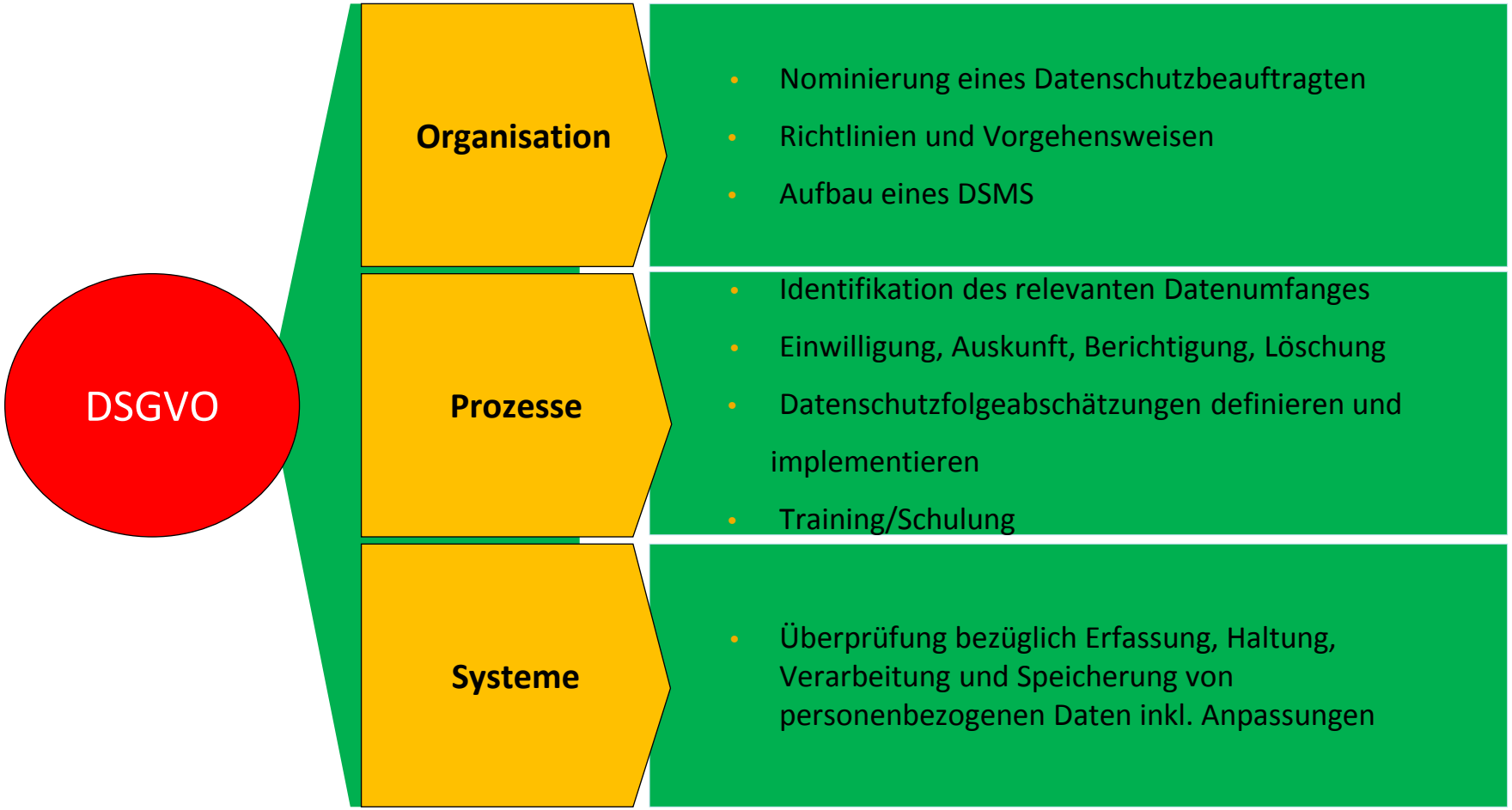
Recht auf Datenübertragbarkeit (Artikel 20)

- Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern :

  - die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

  - die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

3 Säulen-Prinzip



Übersicht über die wichtigsten Dokumente

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

Recht auf Datenübertragbarkeit (Artikel 20)

- Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

Privacy by
design & by default (Artikel 25**)**

Der Verantwortliche muss:

- (1) Einsatz von techn., organ. Maßnahmen (z. B. Pseudonymisierung) die dazu geeignet sind die Datenschutzprinzipien zu gewährleisten, wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen (*Privacy by design*)
- (2) Einsatz von techn., organ. Maßnahmen (z. B. Pseudonymisierung) die dazu geeignet sind die Datenschutzprinzipien zu gewährleisten, über Voreinstellung, dass pbD nur verarbeitet werden, die für den jeweiligen bestimmten Verwendungszweck erforderlich sind. (*Privacy by default*)
- Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Konsequenzen für technische Entwicklungen

Datenschutz und IT-Sicherheit müssen in den Entwicklungsprozess eingebunden werden.

- Der Benutzer muss Eigentümer seiner Daten bleiben.
- Der Benutzer muss darüber informiert sein, was mit seinen Daten geschieht.
- Grundeinstellung aller Verarbeitungen muss sein „data collection off“
- Das Produkt muss auch ohne Einschränkungen und ohne Verarbeitung von pbD arbeiten.
- Starke Authentifizierung ist Vorgabe bei der Verarbeitung pbD.
- Veränderung oder Löschung von Daten durch Unbefugte muss vermieden werden.
- Daten müssen, wenn möglich, pseudonymisiert werden
- Transparenz über alles Gespeicherte, wo es gespeichert ist, wie lange es gespeichert wird und wer ist berechtigt auf die Daten zuzugreifen.
- Konzepte zur Sicherstellung der Aufbewahrungsfristen und zum sicheren Löschen von Daten

Sammeln und Löschen von pbd

- Speichern und Übermitteln nur verschlüsselt
- Verfügbarkeit sicherstellen (wenn notwendig)
- Gespeicherte Daten müssen richtig und aktuell sein.
- Gelöschte Daten dürfen nicht wieder herstellbar sein.
- Die Erlaubnis der Betroffenen ist Bedingung zum Speichern von Daten.
- Daten dürfen nicht bis in alle Ewigkeit gespeichert werden
- Der Betroffene muss die Möglichkeit haben zu jeder Zeit seine Daten löschen zu lassen.

Sicherheit
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

- Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DSGVO kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

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. …

Sicherheit

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.

Erwägungsgrund 78

Geeignete technische und organisatorische Maßnahmen

...

Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

Technikregelungen der Datenschutzgesetze

„Kontrollarten“

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle

- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- zweckbezogene Verarbeitung

„technikoffene Schutzziele“ *

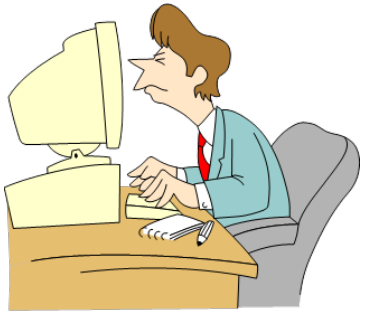
- Verfügbarkeit
- Integrität
- Vertraulichkeit
-
- Transparenz
- Authentizität
- Revisionsfähigkeit
- Nichtverkettbarkeit
- Intervenierbarkeit

- Systemdatenschutz
- Audit / Zertifizierung
- Selbstdatenschutz

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

TOM BDSG-NEU § 64

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zutritts-<u>Zugangskontrolle</u>**)



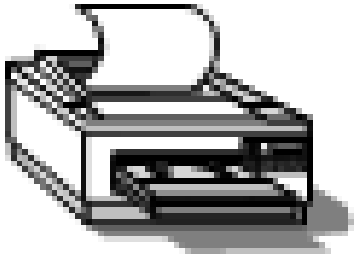
TOM BDSG-NEU § 64

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (**Datenträgerkontrolle**)

TOM BDSG-NEU § 64

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**)

TOM BDSG-NEU § 64



4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**)

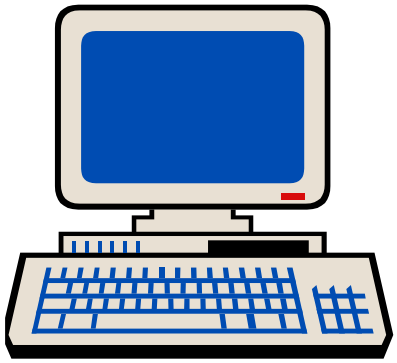
TOM BDSG-NEU § 64

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (**Zugriffskontrolle**)

TOM BDSG-NEU § 64

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personen-bezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**)

TOM BDSG-NEU § 64



7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (**Eingabekontrolle**)

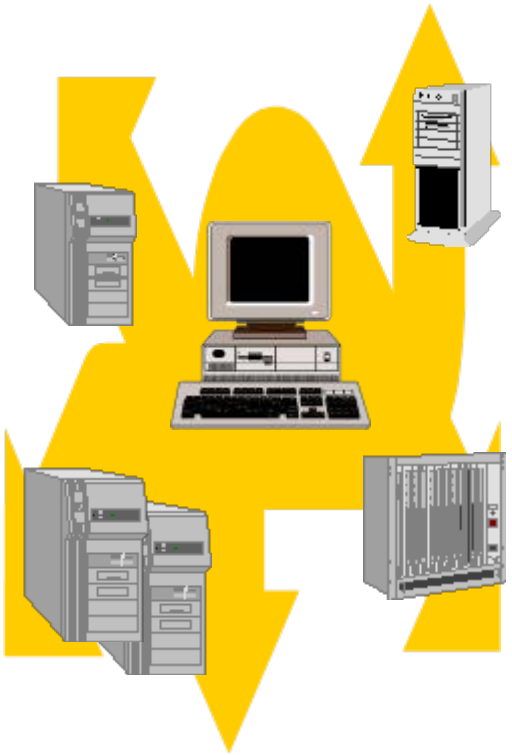
TOM BDSG-NEU § 64

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (**Transportkontrolle**)

TOM BDSG-NEU § 64

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellbarkeit**)

TOM BDSG-NEU § 64

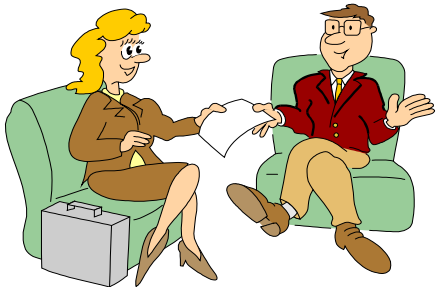


10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**)

TOM BDSG-NEU § 64

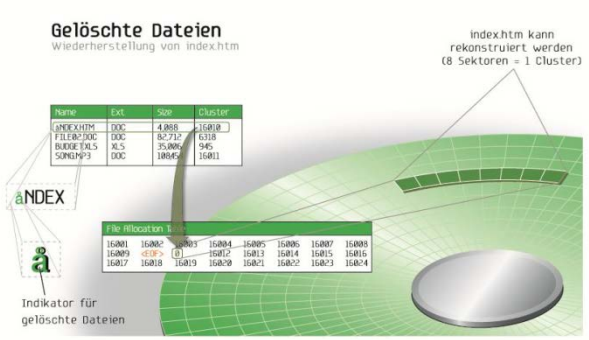
11. Gewährleistung, dass gespeicherte personen-bezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**)

TOM BDSG-NEU § 64



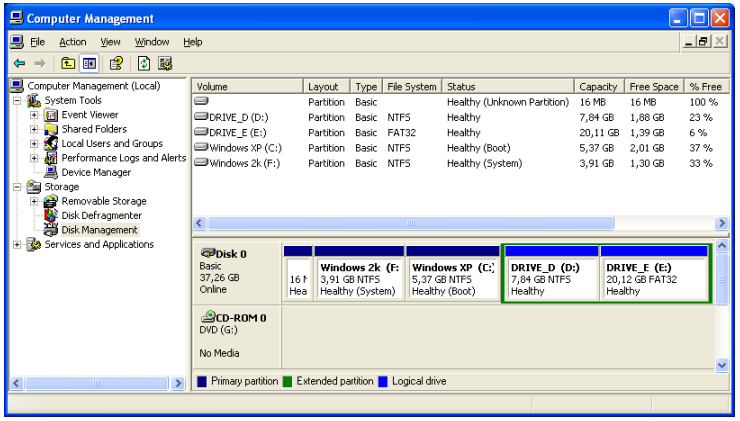
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**)

TOM BDSG-NEU § 64



13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**)

TOM BDSG-NEU § 64

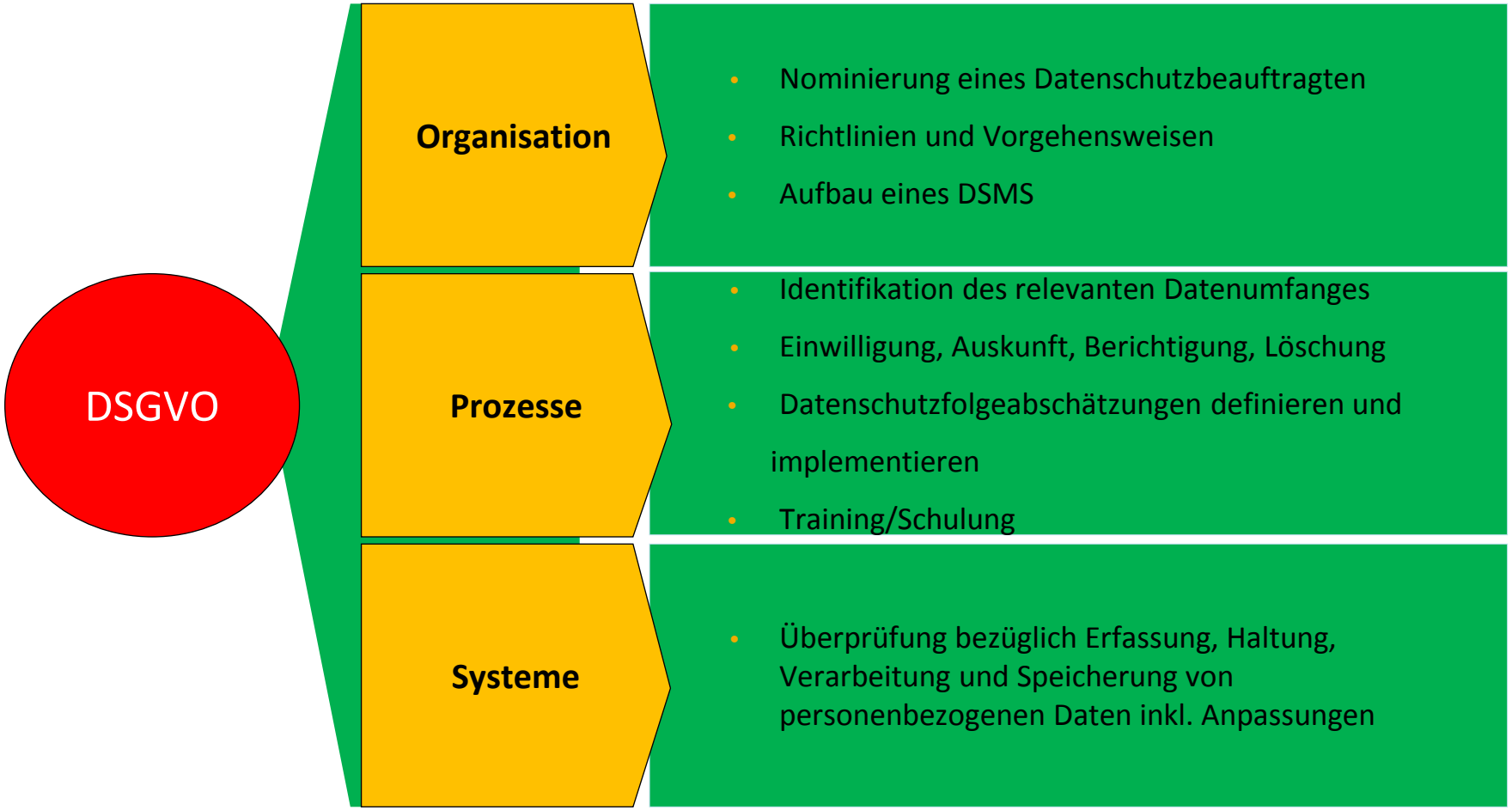


14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (**Trennbarkeit**)

Was ist zu tun???

- DSB benennen
- Prüfung vorhandener Einwilligungserklärungen
- Prüfung der ADV-Verträge auf DS-GVO
- Aufbau der Verfahrensübersichten
- Rechtmäßigkeitsprüfung Verfahren
- Durchführung einer Datenschutz-Folgenabschätzung
- Aufbau und Implementierung eines DSMS
- Anpassung der Systeme an die TOM
- Sicherstellung der Betroffenenrechte

3 Säulen-Prinzip im Fokus



Übersicht über die notwendigen Dokumente

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

Fazit Datenschutz / DSGVO

- ✓ Datenschutz ist Vorstandsangelegenheit / GF-Angelegenheit
- ✓ Es wird komplizierter: „**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

Raum für Diskussion

Jetzt sind Sie dran…

… und zum Schluss

Danke für
Ihre Aufmerksamkeit..