# Die wesentlichen Fakten zur EU-Datenschutz-Grundverordnung - Maßnahmen zur Umsetzung

Rechtsanwalt Markus Giese
Senior Experte Datenschutz DPA GmbH

# Zielsetzung

- Grundkenntnisse zur DSGVO vermitteln
- Anforderungen an die Geschäftsführung aufzeigen
- Handlungsbedarf für Unternehmen und erste Schritte zur Umsetzung der DSGVO aufzeigen

16.12.15 | **Datenschutzreform**

# Europa nimmt Google und Facebook an die Leine

**Die EU hat ihre Datenschutzreform beschlossen, die ab 2018 gilt. Für Internet-Konzerne aus den USA dürfte das unangenehm werden. Aber auch manche WhatsApp-Nutzer müssen bei ihren Eltern "bitte" sagen.** *Von Benedikt Fuest*

Europas Internetnutzer können von 2018 an auf einen besseren Schutz ihrer persönlichen Daten vertrauen. Nach fast vier Jahren Debatten hat die EU eine Datenschutzreform beschlossen, die die Regeln von 1995 ersetzen soll und Google (Link: http://www.welt.de/themen/google/) , Facebook (Link: http://www.welt.de/themen/facebook/) & Co engere Grenzen setzt.

Nutzer erhalten unter anderem das Recht, Informationen leichter wieder löschen zu lassen ("Recht auf Vergessenwerden") (Link: http://www.welt.de/128165702) und Daten von einem Anbieter zum nächsten mitzunehmen ("Portabilität"). Internet-Konzerne müssen die Zustimmung zur Datennutzung ausdrücklich einholen und ihre Produkte datenschutzfreundlich voreinstellen. Die Anbieter müssen den Nutzer auch so schnell wie möglich über Datenlecks informieren.

"EU-Bürger sind künftig Herr über ihre persönlichen Daten", sagte EU-Justizkommissarin Vera Jourova zu dem Kompromiss, den EU-Parlament, EU-Kommission und Staaten ausgehandelt haben. Hat ein Verbraucher ein Problem mit einem Anbieter in einem anderen EU-Land, kann er sich in seiner Sprache an die heimische Beschwerdestelle wenden. Bislang war dies nicht möglich; so musste der Österreicher Max Schrems in Irland gegen Facebook klagen.

# VORGESCHICHTE UND AUSWIRKUNGEN

# Vorgeschichte – Zielsetzung der Novelle

- Vereinheitlichung der Datenschutzbestimmungen innerhalb der EU – derzeit: erhebliche Unterschiede
- Anpassung an Herausforderungen der Digitalisierung (Big Data / Internet der Dinge)
- Erfassung US-amerikanischer Unternehmen: Erstreckung des Anwendungsbereiches auf ausländische Unternehmen, die Daten von EU-Bürgern verarbeiten
- Technikneutrale Ausgestaltung

# Weitergehender Harmonisierungsbedarf besteht!

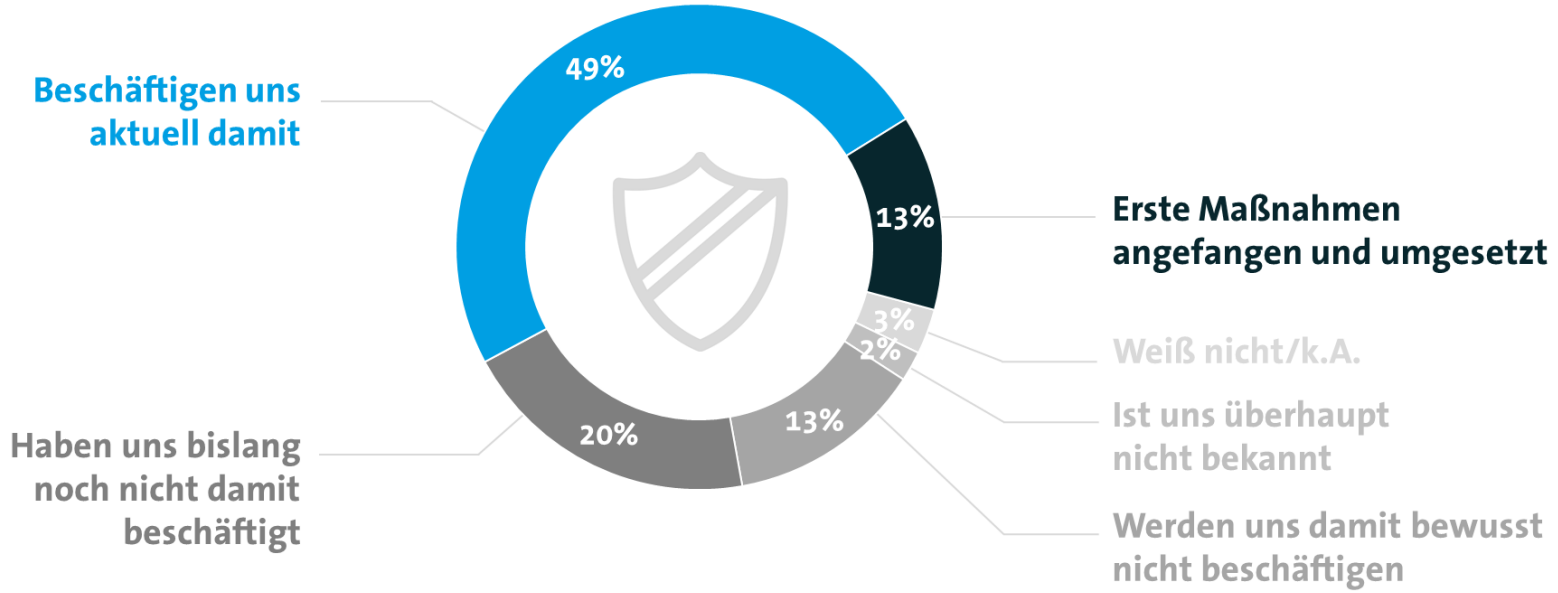
- DSGVO: Direkte Anwendbarkeit ab Mitte 2018
- Anpassungsbedarf im BDSG / TMG:
  - Keine Wiederholungen im nationalen Recht!
- Sonderregelungen im nationalen Recht, sofern Erlaubnis in DSGVO vorhanden; BDSG (neu) Ende April beschlossen
- Zudem: Großer Harmonisierungsbedarf in der EU, da einheitliche Auslegung DSGVO erforderlich. Dies betrifft:
  - Zulässigkeit der Datenverarbeitung
  - Compliance-Anforderungen
  - Ahndung von Verstößen

# Überarbeitung
# DSRL elektronische Kommunikation

- DSRL elektronische Kommunikation betrifft insbesondere elektronisches Marketing:
  - Einsatz von Cookies
  - Marketing mittels E-Mail und Telefon
- Anpassung an die DSGVO erforderlich
- Strengere Vorgaben für Online-Marketing geplant:
  - Endgerät als Teil der Privatsphäre
  - Zugriff grundsätzlich nur mit Einwilligung
  - Zugriff unabhängig davon, ob es sich um personenbezogene Daten handelt
- Sonderregelung für Einwilligung bei Installation von Software geplant

# Jedes dritte Unternehmen ignoriert bislang die DS-GVO

Wie weit ist Ihr Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) zum aktuellen Zeitpunkt?




Basis: Unternehmen ab 20 Mitarbeitern (n=507) | Quelle: Bitkom Research

bitkom

# BASICS – ZENTRALE THEMEN

# Worum geht es beim Datenschutz?

- Alle Datenschutzgesetze sollen den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG)

- Nicht: Schutz von Daten

  *sondern*:

- Schutz der Entscheidungsbefugnis des Einzelnen über die Verwendung seiner Daten

# Wie wird geschützt ?

- **Alle** Datenschutzgesetze folgen dem Grundsatz:

  **Die Verarbeitung personenbezogener Daten ohne ausdrückliche gesetzliche Erlaubnis ist verboten!**

**Keine Rechtsgrundlage**

**=**

**Keine Verarbeitung**

# Gesetzliche Rechtsgrundlage oder Einwilligung?


Einwilligung

**vs.** §§§

Gesetzliche Rechtsgrundlage

- Klare Trennung zwischen Datenverarbeitung auf gesetzlicher Rechtsgrundlage und Verarbeitung aufgrund einer Einwilligung!

# Was wird geschützt ?

- Personenbezogene Daten sind
  - Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren lebenden Person (Betroffener)
  - Auch wenn zunächst nur eine Kennziffer vorhanden ist, diese aber einem Mitarbeiter zugeordnet werden kann, handelt es sich um personenbezogene Daten
  - Nur wenn eine Kennziffer einer natürlichen Person nicht zugeordnet werden kann, handelt es sich um anonyme Daten

# Personenbezug: EuGH Urteil vom 19.10.2016

- Fragestellung:
  - Dynamische IP Adresse als personenbezogenes Datum?
  - Personenbezug aufgrund der Verknüpfbarkeit?
- EuGH:
  - nicht erforderlich, dass die Information für sich genommen die Identifizierung der betreffenden Person ermöglicht
  - nicht alle zur Identifizierung der betreffenden Person erforderlichen Informationen müssen in den Händen einer einzigen Person liegen
  - Personenbezug aufgrund der rechtlich zulässigen Bereitstellung von Daten durch Dritte ausreichend

Schwere Vorwürfe

# Bose Connect-App soll Nutzer ausspionieren


**Die Audio-Experten von Bose haben einen handfesten Skandal am Hals. Bose-Kopfhörer sollen Informationen über abgespielte Musik an Bose und eine Data-Mining-Firma weitergeben. Anonymisiert seien die Daten auch nicht. Die Empörung ist groß, aber Bose hat seine Noise-Cancelling-Kopfhörer aufgesetzt.**


## Nichts ist uns wichtiger als Ihr Vertrauen.

Seit über 50 Jahren arbeiten wir unermüdlich daran, uns dieses Vertrauen zu verdienen und es zu bewahren. Daran hat sich nichts geändert und es wird sich auch nichts daran ändern.

Um bei der ständigen Verbesserung unserer Produkte und Services sowie bei der Fehlerbehebung zu helfen, erfasst Bose Connect Diagnose- und Nutzungsdaten. Sollten Sie die Erfassung dieser Daten nicht wünschen, können Sie in der App unter „Datenschutz“ entsprechende Einstellungen vornehmen.

OK

# Personenbezug von Daten

- Bislang: sehr umstritten, wie Personenbezug von Daten zu bestimmen ist
- DSGVO:
  - Weite Definition festgeschrieben („Single Out“)
  - Übernahme der Position der Art. 29 Gruppe
- Auch IP-Adressen, Cookie-IDs oder sonstige Identifier sind personenbeziehbar, sofern hierzu weitere Daten gespeichert werden (EG 30 und Art. 4 Abs. 1).
- Massive Auswirkungen für Datenverarbeitung im Internet und für Datenanalyse

**Wir weisen darauf hin, dass ein Personenbezug von rein technischen Daten (wie etwa Auslesen des Gurtstrafferstatus) besteht, sobald das Datum mit der Fahrzeugidentifikationsnummer oder einem sonstigen Identifikationsmerkmal verknüpft ist.**

# Datenschutzprinzipien – von Unternehmen immer zu beachten!

- Verschärfung der bestehenden Regelungen [Art. 5 (1)]:
  - Gesetzeskonforme, faire und transparente Datenverarbeitung
  - Zweckbindung und Zweckänderung
  - Datensparsamkeit
  - Zeitlich begrenzte Speicherung
  - Vertraulichkeit und Integrität der Daten
- Accountability (Art. 5 Abs. 2): Nachweis zur Umsetzung gefordert
- Bußgeld: bis zu 20 MIO EUR oder 4 % des Jahresumsatzes der Gruppe

# Zur Zweckbindung

- Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden, Art. 5 Abs. 1 lit. b und c
- **Information** über Verwendungszweck bei Datenerhebung
- Erhebung zu nicht bestimmten Zwecken ist unzulässig (**keine Vorratsdatenspeicherung**)
- Mit Zweckerreichung besteht Löschungspflicht!
- Data LifeCycle Management gefordert

# Zulässigkeit einer Zweckänderung

- Zweckänderung (auch) auf Grundlage der Interessenabwägungsklausel zulässig:
  - der neue Zweck muss mit dem bisherigen Zweck vereinbar sein
  - Datenverarbeitung für neuen Zweck muss auf Rechtsgrundlage gestützt werden können
  - Information des Betroffenen über neuen Verwendungszweck erforderlich
- Zudem: Zweckänderung nach § 24 BDSG n. F. zulässig:
  - zur Abwehr von Gefahren für öffentliche Sicherheit oder zur Verfolgung von Straftaten
  - zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich

# Einwilligung in die Datenverarbeitung

- Folgende Erfordernisse müssen nach DSGVO beachtet werden (Art. 6 Abs. 1 lit. a, Art. 7):
  - Eindeutige Willensbetätigung des Betroffenen („*unambiguous*“, nicht „*explicit*“),
  - klare und eindeutige Formulierung der Einwilligung
  - Freiwillige Zustimmung; separates Anklicken/ Zustimmung zur Datenverarbeitung
  - Einführung Kopplungsverbot (kein „Payback-Modell“)
  - Nachweispflicht beachten!
- Anforderungen im Rahmen der Verhandlungen sehr umstritten!

# Begrenztes Kopplungsverbot neu eingeführt

- Mit DSGVO umfassendes Kopplungsverbot eingeführt
- Bislang „take it or leave it“ zulässig, künftig verboten!

- Vermutungsregel (EG 43):
  „Die Einwilligung gilt nicht als ohne Zwang erteilt, wenn zu verschiedenen Datenverarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig gemacht wird, obwohl dies für diese Erfüllung nicht erforderlich ist.“

# Zentralisierung der Datenverarbeitung künftig begrenzt möglich

- Einführung eines „kleinen Konzernprivilegs“;
  kein umfassendes Konzernprivileg
  - Zentralisierung der Datenverarbeitung zulässig
  - Relevant für Mitarbeiterdaten

- Joint-Controllers:
  - häufiger anwendbar, als gedacht
  - Präzisierung der Anforderungen
  - Siehe auch Positionspapier Art. 29 Gruppe

# ZULÄSSIGKEIT DER DATENVERARBEITUNG

# Zulässigkeitsanforderungen im Überblick

- Allgemeines Vorgaben zur Zulässigkeit der Datenverarbeitung in Art. 5 („Grundsätze der Datenverarbeitung“)

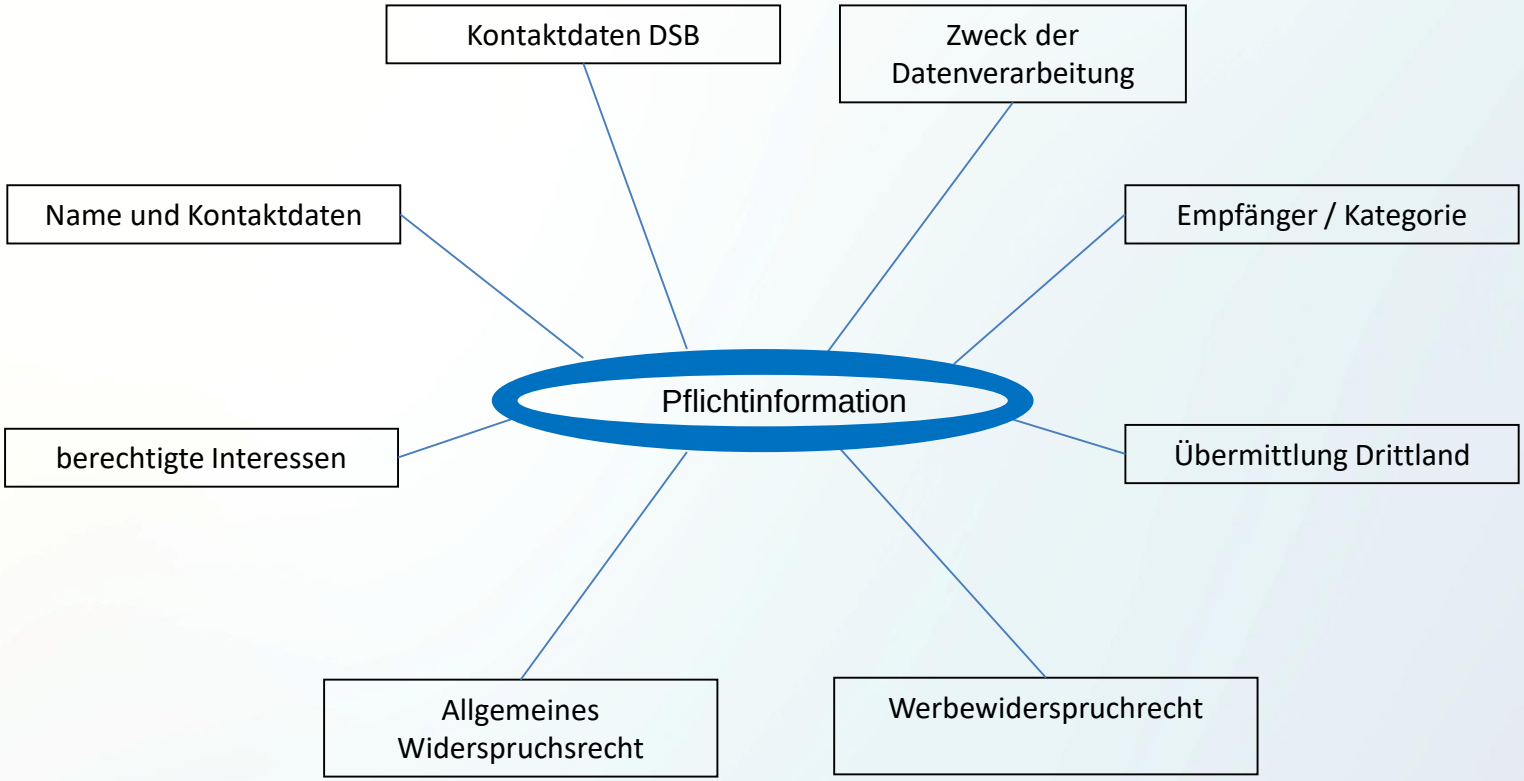
- Folgende Prinzipien sind zu beachten:
  - Transparenz
  - Rechtmäßigkeit
  - Zweckbindung
  - Erforderlichkeit / Datenminimierung

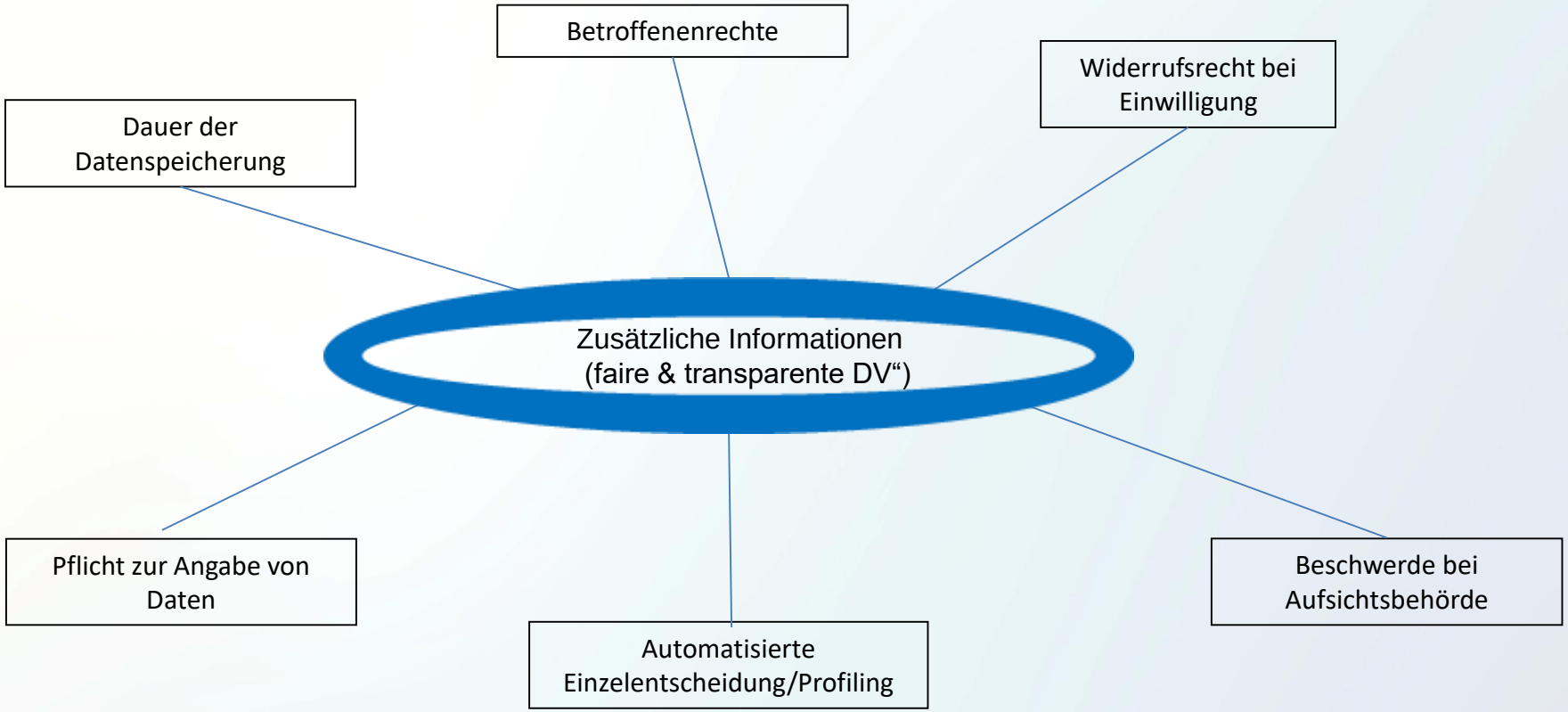
# Einschlägige Rechtsgrundlagen

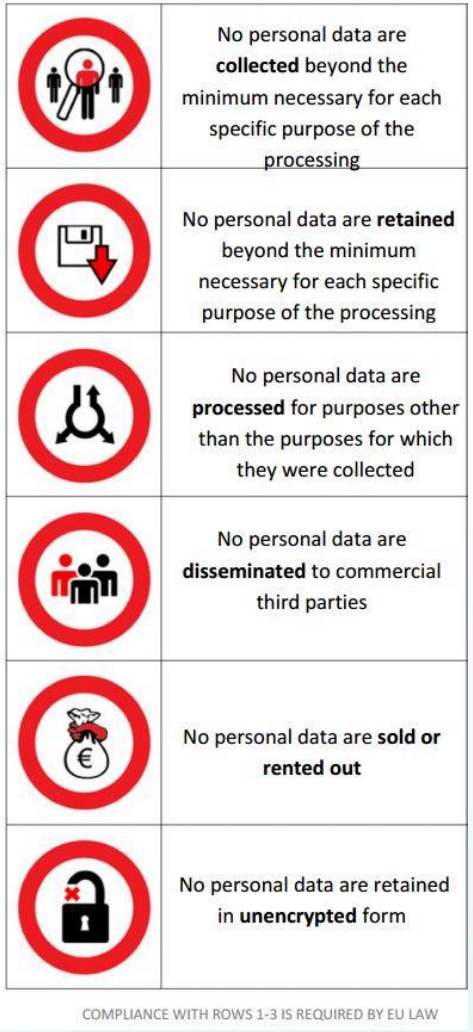
- Datenverarbeitung zur Erfüllung eines Vertrags erforderlich; auch vorvertragliche Maßnahmen erfasst.
- Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der das Unternehmen unterliegt
- Datenverarbeitung auf Grundlage der Interessenabwägungsklausel
  - Berechtigte Interessen des Unternehmens / eines Dritten erfordern die Datenverarbeitung
  - Interessen der Betroffenen dürfen nicht überwiegen
- Einwilligung des Betroffenen

# Informationspflichten – Überblick

- Sehr umfangreiche Informationspflichten vorgesehen, Art. 12 ff.
- Transparenzpflicht = Kernanliegen der DSGVO;
- Massive Stärkung / Ausweitung des Transparenzprinzips
- Auswirkungen auf Zulässigkeit der Datenverarbeitung
- Verstoß: Geldbuße bis zu 20 MIO EUR


Kontaktdaten DSB
Zweck der Datenverarbeitung
Name und Kontaktdaten
Empfänger / Kategorie
Pflichtinformation
berechtigte Interessen
Übermittlung Drittland
Allgemeines Widerspruchsrecht
Werbewiderspruchrecht


Betroffenenrechte
Widerrufsrecht bei Einwilligung
Dauer der Datenspeicherung
Zusätzliche Informationen (faire & transparente DV“)
Pflicht zur Angabe von Daten
Automatisierte Einzelentscheidung/Profiling
Beschwerde bei Aufsichtsbehörde




## Vorschlag Icons (EU-Parlament); finale Vorgaben erfolgen durch EU-Kommission

# BESCHÄFTIGTENDATENSCHUTZ

# Öffnungsklausel im Beschäftigtendatenschutz

- Detaillierte Regelungen zum BeschDS fehlen in der DSGVO
- Öffnungsklausel für Regelungen in Mitgliedstaaten in Art. 88 DSGVO vorhanden
- BeschDS bleibt eine Domäne der Mitgliedstaaten, aber unklar,
  - ob nur Präzisierungen erfolgen dürfen
  - oder ob auch Verschärfungen zulässig sind
- Jedenfalls:
  - Allgemeine Grundsätze gelten (Art. 5 DSGVO)
  - Mitarbeiter können sich auf Betroffenenrechte berufen

# Art. 88 Abs.1 – Datenverarbeitung im Beschäftigungskontext

*„Die Mitgliedstaaten können durch **Rechtsvorschriften** oder durch **Kollektivvereinbarungen** spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten…“*

**Rechtsgrundlagen der Verarbeitung von Beschäftigtendaten**

- § 26 BDSG neu
- Betriebsvereinbarungen

# § 26 BDSG neu

- **Abs.1:** gesetzliche Grundlage
  - für Zwecke des Beschäftigungsverhältnisses; Aufdeckung von Straftaten
- **Abs.2:** Grundlage Einwilligung
  - Freiwilligkeit, Schriftform; Informationen über Zweck und Widerrufsrecht in Textform
- **Abs.3:** Verarbeitung sensibler Daten
  - rechtliche Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes
- **Abs.4:** Verarbeitung sensibler Daten auch auf Grundlage von Kollektivvereinbarungen zulässig
- **Abs.5:** Beachtung der Grundsätze nach Art. 5 DSGVO (allgemeine Grundsätze)
- **Abs.6:** Beteiligungsrecht der Interessenvertretungen bleiben unberührt

# Art. 88 Abs.2 - Anforderungen an Betriebsvereinbarungen

*„Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.“*

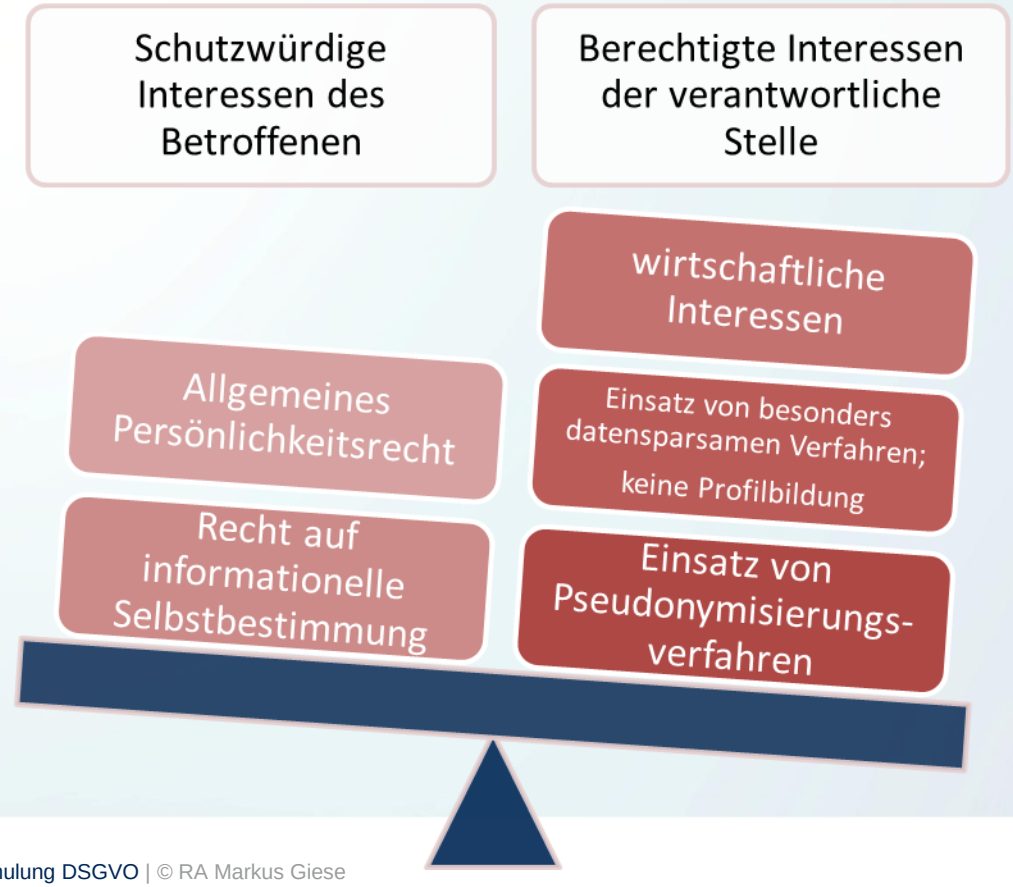
- Weitergehende Anforderungen als bislang von Rechtsprechung aufgestellt worden sind. (Sicherstellung der menschlichen Würde, Transparenzerfordernisse bei Übermittlung im Konzern, Überwachungssysteme am Arbeitsplatz.)
- Zentrale Grundsätze der DSGVO müssen abgebildet werden
- **Ziel:** Absenkung der Datenschutzstandards durch Regelungen Mitgliedstaaten verhindern.

# WERBLICHE NUTZUNG VON DATEN

# Zur Interessenabwägung – ein Überblick

- Weiterhin maßgebliche Rechtsgrundlage für eine Datenverarbeitung für Marketingzwecke
- **Aber:** Begrenzung durch Erwägungsgründe vorgesehen:
  - „Vernünftige Erwartungen“ des Betroffenen
  - Vorgabe zu „berechtigte Interessen“: sollen etwa im Rahmen einer Geschäftsbeziehung vorliegen
- Orientierung an Vorgaben Artikel 29 Gruppe (WP 217)
- Genaue Bestimmung der berechtigten Interessen erforderlich!
- Offen: Welche Auswirkungen bestehen auf die Zulässigkeit der Datenverarbeitung?

# Zur Interessenabwägung – Dokumentationspflicht beachten!



# Unter welchen Voraussetzungen sind die Werbeformen erlaubt?

| Bereich | Opt-In | Kein Opt-In |
|---|---|---|
| Email & Telefonwerbung | ✓ | |
| Schriftliche Werbung | | ✓ |
| Werbescoring | | ✓ |
| Adressmiete | | ✓ |
| Adresskauf/-handel | | ✓ |
| Allg. zugängliche Quelle | | ✓ |

# COMPLIANCEPFLICHTEN NACH DER DSGVO

# Compliance-Anforderungen im Überblick

- Grundsatz der Rechenschaftspflicht, Art. 5 Abs. 2; Art. 22
- [Data Protection by desgin / by default, Art. 25]
- Data Protection Impact Assessment, Art. 35, Art. 36
- [Bestellung eines Datenschutzbeauftragten, Art. 37]
- Verfahrensverzeichnis, Art. 30
- Data breach notification, Art. 33 und 34
- Umsetzung Betroffenenrechte, Art. 12 ff.

# Verzeichnis von Datenverarbeitungen (Art. 30)

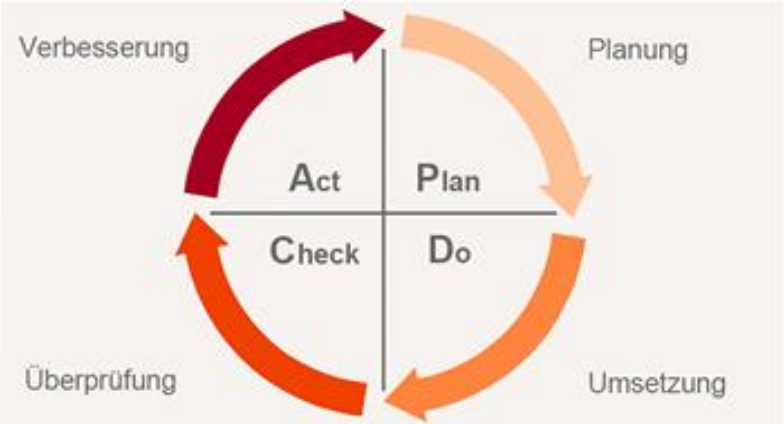
- Verantwortliche müssen wie bisher eine Übersicht zu allen Datenverarbeitungen führen (Art. 30)
- Dienstleister müssen eine (reduzierte) Verarbeitungsübersicht hinsichtlich der für Auftraggeber durchgeführten Datenverarbeitungen vorhalten (Kategorien von Datenverarbeitungen)
- Keine Einsichtnahme durch Öffentlichkeit mehr
- Aufsichtsbehörde hat Einsichtsrecht
- Bußgeld: bis zu 10 MIO Eur. / 2% weltweiter Jahresumsatz
- Interner Regelungsbedarf:
  - Dokumentation der Verfahren
  - Prozess etablieren, damit künftig alle neuen Verfahren / Änderungen erfasst werden.

# Zur Rechenschaftspflicht

- Unternehmen müssen nachweisen können, dass Daten gemäß den Vorgaben der Datenschutzverordnung verarbeitet werden
- Der Erlass von internen Richtlinien ist erforderlich, sofern dies verhältnismäßig ist im Hinblick auf die Datenverarbeitung
- Complianceprozess erforderlich: Review und Aktualisierung der Vorgaben sind geboten
- Nachweis kann durch entsprechende Zertifikate erfolgen

# Klassischer Compliance-Prozess erforderlich

- Regelmäßiger Ablauf:




- und die Dokumentation nicht vergessen!!

# Datenschutz-Handbuch

- Umfassende Zusammenstellung aller Vorgaben zum Datenschutz
  - Organisationsanweisung-Anweisung zum Datenschutz
  - Verantwortlichkeiten für Datenschutz
  - Vertragsmuster (ADV)
  - Richtlinien Umgang Datenverlust
  - Durchführung interner Kontrollen
  - etc.

- Zudem: Bestellungsurkunde Datenschutzbeauftragter & Tätigkeitsberichte

# Dokumentation von Datenverarbeitung & Rechtmäßigkeit

- Dokumentation sämtlicher Datenverarbeitungen gefordert
- Ausführungen zur Rechtmäßigkeit erforderlich, d.h.
  - Beachtung Informationspflichten
  - Durchführung Interessenabwägung
  - Erforderlichkeit eines DPIA
  - Durchführung eines DPIA
  - Beachtung Systemdatenschutz

# Verantwortlichkeiten & Kontrollen regeln!

Unternehmen /
GF & Führungskräfte

- Verantwortlichkeit für Einhaltung des Datenschutzes liegt bei Geschäftsführung

Internes QM / Revision /
Compliance Management

- Interne Kontrollen einführen; Compliance-Prozess
- Datenschutz als Bestandteil des QM

Datenschutzbeauftragter

- Supervision / ergänzende Kontrolle und Beratung durch den DSB

# Weisungsgebundenheit Mitarbeiter beachten!

- Bisher:
  - Strikte Weisungsgebundenheit bei Dienstleistern / Auftragsdatenverarbeitung
  - Erteilung entsprechender Weisungen erforderlich
- NEU:
  - Unternehmen muss sicherstellen, dass Mitarbeiter Daten nur auf Anweisung verarbeiten!
  - Erteilung & interne Dokumentation von Weisungen erforderlich (Art. 32 Abs. 4 DSGVO)

# Data Protection Impact Assessment (Art. 35f.)

- Erforderlich, sofern hohes Risiko für die Rechte der Betroffenen aufgrund der Datenverarbeitung vorliegt
- Einbeziehung des DSB (sofern bestellt)
- Anwendungsfälle sind etwa
  - die systematische und intensive Bewertung von Aspekten eines Betroffenen im Rahmen von automatisierten Datenverarbeitungen, einschließlich Profilbildung
  - Videoüberwachung
- Aufsichtsbehörden sollen Positiv- bzw. Negativlisten für Anwendungsfälle erstellen

# DATENSICHERHEIT

# Vorgaben der DSGVO zur Datensicherheit

Zu gebotenen Maßnahmen zählen (Art. 32 Abs. 1):

- Pseudonymisierung und Verschlüsselung
- Die Sicherstellung einer Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Systeme
- Die Möglichkeit, die Verfügbarkeit und den Zugriff auf Daten bei einem techn. Zwischenfall rasch zu gewährleisten
- Wirksame Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen

# DATA BREACH NOTIFICATION

# Umfassende Meldepflicht

- Personal Data Breach – Verletzung der Datensicherheit, die zu dem zufälligen oder unrechtmäßigen Verlust von Daten führt, Art. 33 und 34
- Auch unberechtigte Weitergabe oder Einsichtnahme ist erfasst.
- Alle Data Breaches müssen der Aufsichtsbehörde gemeldet werden, es sei denn, sie führen nicht zu einem Risiko für die Rechte der Betroffenen
- Umgehende Meldung erforderlich; spätestens innerhalb von 72 h (Ausnahme bei besonderen Umständen)

# Folgende Informationen sind mitzuteilen:

- Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze
- den **Namen und die Kontaktdaten des Datenschutzbeauftragten** oder eines sonstigen Ansprechpartners für weitere Informationen
- eine **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von dem für die Verarbeitung Verantwortlichen **ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung** der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen nachteiligen Auswirkungen

# Interne Dokumentationspflicht

- Unternehmen müssen sämtliche (!) Data Breaches erfassen und dokumentieren (auch nicht meldepflichtige Zwischenfälle)
- Dokumentation umfasst alle im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen
- Dokumentation muss zur Einsichtnahme der Aufsichtsbehörden bereitliegen, um die Einhaltung der Vorgaben zu prüfen
- Verstoß: Bußgeld bis zu 10 MIO EUR

# Kommunikation gegenüber Betroffenen

- Nur sofern ein **hohes Risiko** für die Rechte der Betroffenen vorliegt, muss eine Information folgen
- DSGVO enthält Ausnahmeregelungen:
  - Geeignete technische Schutzmaßnahmen wurden angewandt, etwa Verschlüsselung der Daten
  - durch nachträglich ergriffene Maßnahmen besteht kein hohes Risiko mehr
- Bei hohem Aufwand: öffentliche Bekanntmachung gefordert
- Inhalt der Informationspflicht ist gleich (Art. 34 (3) DSGVO)
- Verstoß: Bußgeld bis zu 10 MIO EUR

# BEAUFTRAGUNG EXTERNER DIENSTLEISTER

# Inhaltliche Anforderungen an ADV-Vertrag

- Vergleichbare (aber nicht identische) Regelung wie zu § 11 BDSG eingeführt
- Vertrag muss bestimmte inhaltliche Kriterien erfüllen, u.a.:
  - Gegenstand der Datenverarbeitung
  - Dauer, Zweck und Art der Datenverarbeitung
  - Datenkategorien und Betroffenen
  - Regelung zur Beauftragung von Subdienstleistern
  - Einführung Verschwiegenheitspflicht für alle Mitarbeiter / angemessene gesetzliche Verschwiegenheitspflicht
  - alle erforderlichen Vorgaben zur IT-Sicherheit (Art. 32)

# Kontrollen des Auftraggebers

- Auftraggeber muss sich überzeugen, dass Einhaltung der Vorgaben gewährleistet ist
- Keine Vorabkontrolle mehr vorgesehen
- Der Dienstleister muss gegenüber dem Auftraggeber alle Informationen liefern, um die Einhaltung der Vorgaben des Vertrags nachzuweisen. Entsprechende Überprüfungen durch den Auftraggeber sollen ermöglicht werden.
- Nachweis der hinreichenden Garantien kann zur Zertifikate vereinfacht werden

-> Compliance-Aufgabe für Unternehmen

# Anpassungsbedarf bestehender Verträge

- Verträge müssen ergänzt und angepasst werden
- Überzeugungsbildung gefordert
  - Checklisten entwerfen
  - Vor-Ort-Kontrollen durchführen
  - Dokumentation erforderlich
- Fernwartung: nicht von Definition der ADV erfasst

# Zur Zusammenarbeit mit dem Auftraggeber

- Gesamtschuldnerische Haftung gesetzlich angeordnet
- Prozesse müssen definiert werden
  - Umsetzung Meldepflicht bei Datenverlust
  - Sicherer Datentransfer zum Auftraggeber
  - Umsetzung Betroffenenrechte (z.B. Auskunftsanspruch)
- Regelmäßige interne Kontrollen des Dienstleisters erforderlich:
  - Betrifft IT-Sicherheit
  - Weisungsgebundenheit Mitarbeiter
  - Durchführung von Schulungen

# BETROFFENENRECHTE

# Betroffenenrechte - Zielsetzung

- Zielsetzung: Stärkung der Betroffenenrechte, um dem Betroffenen weitergehende Kontrolle über ihre Daten zu sichern
  - Einführung neuer Rechte (Recht auf Vergessenwerden; Datenportabilität)
  - bei Verstoß: Bußgeld bis 20 MIO EUR
- Controller müssen entsprechende Prozesse etablieren, um Anfragen zu beantworten & Umsetzung nachzuhalten

# Recht auf Löschung / „Vergessenwerden“

- Klassisches Recht auf Löschung in Art. 17 Abs. 1, einschließlich Widerspruch des Betroffenen gegen die Datenverarbeitung
- Sonderregelung zur Löschungspflicht in Art. 17 Abs. 2a im Fall der Veröffentlichung:
  - Informationspflicht gegenüber anderen verantwortlichen Stellen über Löschungspflicht von Links / Kopien / Replikationen von Daten
  - Einschränkungen können sich aus verfügbarer Technologie / Implementierungskosten ergeben
- Ausnahme von Löschpflicht  Art. 17 (3):
  - Freie Meinungsäußerung
  - Archivzwecke etc.

# Recht auf „*Einschränkung der Verarbeitung*“

- Entspricht weitgehend der Sperrung von Daten
- Liegt etwa vor, wenn Daten nicht mehr für Zweckerreichung benötigt werden, die betroffene Person sie aber zur Geltendmachung / Ausübung oder Verteidigung von Rechtsansprüchen benötigt
- Daten dürfen nur mit Einwilligung, zur Geltendmachung / Ausübung oder Verteidigung von Rechten oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden

# Recht auf Datenportabilität

- Anspruch auf Herausgabe von Daten in einem strukturierten gängigen und maschinenlesbaren Format
- Alternative: Recht auf direkte Weitergabe an einen anderen Diensteanbieter, sofern technisch machbar
- Voraussetzung: Datenverarbeitung erfolgt
  - auf Grundlage einer Einwilligung oder
  - auf Grundlage eines Vertrages
  - Betroffener muss Daten bereitgestellt haben
- Unternehmen müssen entsprechende Maßnahmen treffen, um Datentransfer zu ermöglichen (Art. 20)

# Auskunftsrechte

- Detaillierte Regelung in Art. 15;
  entspricht weitgehend der bekannten Regelung in § 34 BDSG
- Auskunftsrecht umfasst u.a. folgende Punkte:
  - Verwendungszwecke
  - Empfänger der Daten
  - Herkunft, sofern Daten nicht beim Betroffenen erhoben
  - Aussagen zur Dauer der Speicherung / Nutzung
  - Hinweise zum Recht auf Löschung / Beschwerderecht bei Aufsichtsbehörde
  - Detaillierte Angaben im Fall des Profilings (Aussagen zu Logik; Tragweite und angestrebte Auswirkungen)

# Recht auf Kopie

- Betroffene kann nach Art. 15 Abs. 3 eine Kopie der Daten verlangen, die Gegenstand der Verarbeitung sind.
- Ziel: Betroffene soll sich – zusammen mit den weiteren Informationen – von der Zulässigkeit der Datenverarbeitung überzeugen können.
- Offen: was ist mit Daten, die archiviert worden sind?

# Widerspruchsrecht (Art. 19)

- Allgemeines Widerspruchsrecht aus überwiegenden Gründen des Betroffenen in Art. 21 Abs. 1
  - Betrifft Gründe aus der besonderen Situation des Betroffenen
  - Führt zu Verarbeitungsverbot für Controller; Ausnahme: zwingende Gründe überwiegen Interessen des Betroffenen
- Spezifisches Widerspruchsrecht für Direktmarketing / Profiling für Werbezwecke /
  - Keine Angabe von Gründen

# AUFSICHTSBEHÖRDEN, STRAFEN UND HAFTUNG

# Aufgaben der Aufsichtsbehörden

- Müssen die Einhaltung der DSGVO überwachen & durchsetzen, Art. 57
- Pflicht zur Abstimmung / Zusammenarbeit (Kohärenzverfahren, Art. 60, 63), um **einheitliche Anwendung** zu gewährleisten

-> Ganz neue Anforderungen an die Arbeit von Aufsichtsbehörden

-> Offen: Fortbestand des Düsseldorfer Kreises

# Abhilfebefugnisse - Ahndung von Verstößen

- Abhilfebefugnisse nach Art 53 Abs. 1b umfassen u.a.:
  - Verwarnung
  - Anweisung, Anfragen von Betroffenen zu beantworten
  - Anordnungen zu treffen, Datenverarbeitung so zu gestalten, dass sie den Vorgaben der DSGVO entspricht
  - Untersagung einer Datenverarbeitung
  - Entzug eines Datenschutzsiegels
  - Untersagung eines Datentransfers außerhalb der EU
  - Geldbuße nach Art. 83 (zusätzlich / anstelle)

# Geldbußen - allgemeine Vorgaben

- Vorgaben in Art. 83:
  - Bußgelder müssen *wirksam, verhältnismäßig* und *abschreckend* sein
  - Bußgelder sollten bei Verstößen ausgeworfen werden, Verzicht auf Bußgeld nur bei geringen Verstößen (EG 148)
  - es besteht begrenzter Ermessensspielraum der Aufsichtsbehörde, ob Bußgeld verhangen wird
  - Vorgaben zur einheitlichen Anwendung des Bußgeldrahmens in der EU vorgesehen

# Bußgeld - Vorgaben für Bemessung

Folgende Punkte sind u.a. bei der Bemessung des Bußgeldes zu berücksichtigen:

- Art, Schwere und Dauer des Verstoßes
- der vorsätzliche Charakter
- Maßnahmen zur Minderung des entstandenen Schadens
- der Grad der Verantwortlichkeit
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde
- Umfang der Zusammenarbeit mit Aufsichtsbehörden

# Bußgeldrahmen (I)
# bis zu 10 MIO

- Bußgeldrahmen bis zu 10 Mio. Euro
  (bzw. 2 % des weltweiten Jahresumsatzes der Unternehmensgruppe)
- folgenden Regelungen z.B. betroffen:
  - Führung eines Verfahrensverzeichnisses
  - Bedingungen für Einwilligung von Kindern
  - Vorgaben Datensparsamkeit / privacy by design / PIA
  - Vorgaben Joint controllership
  - Regelungen Auftragsdatenverarbeitung
  - Zusammenarbeit mit Aufsichtsbehörden
  - Sicherheit Datenverarbeitung
  - Meldepflichten („Data Breach Notification“)

# Bußgeldrahmen (II) – bis zu EUR 20 Mio.

- Bußgeld bis zu 20 Mio. Euro (bzw. 4 % weltweiter Jahresumsatz der Unternehmensgruppe) bei Verletzung
  - von grundlegenden Prinzipien des Datenschutz,
  - Speziell: fehlende Zulässigkeit der Datenverarbeitung
  - der Verletzung von Betroffenenrecht
  - Vorgaben zum Datentransfer außerhalb EU
  - bei Missachtung von Vorgaben der Aufsichtsbehörden

# Bußgelder – Stellungnahme Aufsichtsbehörde

**Ausblick zu drohenden Bußgeldern**

Aus den Sanktionsvorschriften der DS-GVO spricht der deutliche Wille des Gesetzgebers, Datenschutzverstöße konsequent und bei Bedarf auch empfindlich zu ahnden. Dies ist ein deutliches Signal, dass sich eine Inkaufnahme von Datenschutzverstößen nicht lohnt.

Unternehmen müssen den Datenschutz daher zwangsläufig noch mehr als bisher in den Fokus ihrer eigenen Aufmerksamkeit nehmen.

# DIE ERSTEN SCHRITTE – UMSETZUNG DER DSGVO

# **Ablauf** der unternehmensinternen Umsetzung (Überblick)

- **Phase 1:** Information an Geschäftsführung;
  Benennung Projektteam; Benennung Datenschutzkoordinator
- **Phase 2:** Erfassung und Bewertung
  - unternehmensinterne Erfassung sämtlicher Datenverarbeitungen
  - datenschutzrechtliche Bewertung („GAP-Analyse“)
  - Entscheidung Geschäftsführung zur Realisierung der einzelnen Umsetzungsschritte
- **Phase 3:** Realisierungsphase
  - Anpassung bestehender Prozesse
  - Rollout-Datenschutzmanagement

# 1. Phase: Zum Projektteam

- Mitglieder des Projektteams
  - sind aus jedem relevanten Fachbereich erforderlich
  - werden durch GF / verantwortliche Führungskraft benannt
- Aufgaben der Mitglieder des Projektteams:
  - Kommunikation der Anforderungen in den Fachbereichen
  - Rückmeldung / Zulieferung aus dem Fachbereich in das Projektteam
  - Begleitung der Umsetzung in den Fachbereichen

# 2. Phase: Erfassung der relevanten Datenverarbeitungen

- Zulieferung von relevanten Informationen zur praktizierten Datenverarbeitung durch Fachbereich
- Orientierung an dem bisherigen Verfahrensverzeichnis
- Erfassung der relevanten Datenverarbeitungen mittels Fragebogen / Interview

# 2. Phase:
# GAP-Analyse & Entscheidung GF

- Ablauf GAP-Analyse wie folgt:
  - Ermittlung der relevanten Anforderungen aus der DSGVO
  - Bewertung, in welchem Umfang Handlungsbedarf vorliegt
- Ergebnis:
  - Bericht zum konkreten Handlungsbedarf
  - Matrix mit Risikobewertung
  - Priorisierung der anstehenden Aufgaben (Vorschlag)
  - Entscheidung der GF über die Realisierung

# Phase 3:
## Einführung organisatorischer Vorgaben

- Einführung / Ausbau eines Datenschutzmanagement
  - Erarbeitung interner Arbeitsanweisungen zum Datenschutz
  - Überprüfung von Verantwortlichkeiten / Ressourcen
  - Anpassung weiterer Arbeitsanweisungen / Verzahnung mit IT-Governance
- Einführung von Wirksamkeitskontrollen zur Einhaltung der Datenschutzvorgaben / Reporting
- Schulung der Führungskräfte

# Phase 3:
## Umsetzung übergreifender Aspekte

Beispielhaft folgende Punkte zu benennen:

- Regelung zum Umgang mit einem Datenverlust („data breach notification“)
- Umsetzung zentraler Vorgaben, etwa
  - Archivierungs- und Löschkonzept
  - Umsetzung neuer Betroffenenrechte

# Phase 3:
## Umsetzung in einzelnen Abteilungen

Folgende Aufgaben stehen an:

- Anpassung von Verfahren gemäß GAP-Analyse
  - Anpassungen von Informationsklauseln / Musterschreiben
  - Anpassungen in der IT
- Dokumentation der Verfahren
  - Ablauf der Datenverarbeitung
  - Rechtmäßigkeit der einzelnen Verfahren
- Schulung der Mitarbeiter

# Die Verursacher…