HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Neues Datenschutzrecht: Die EU-Datenschutz-Grundverordnung

HECKER WERNER HIMMELREICH
Rechtsanwälte Partnerschaft mbB

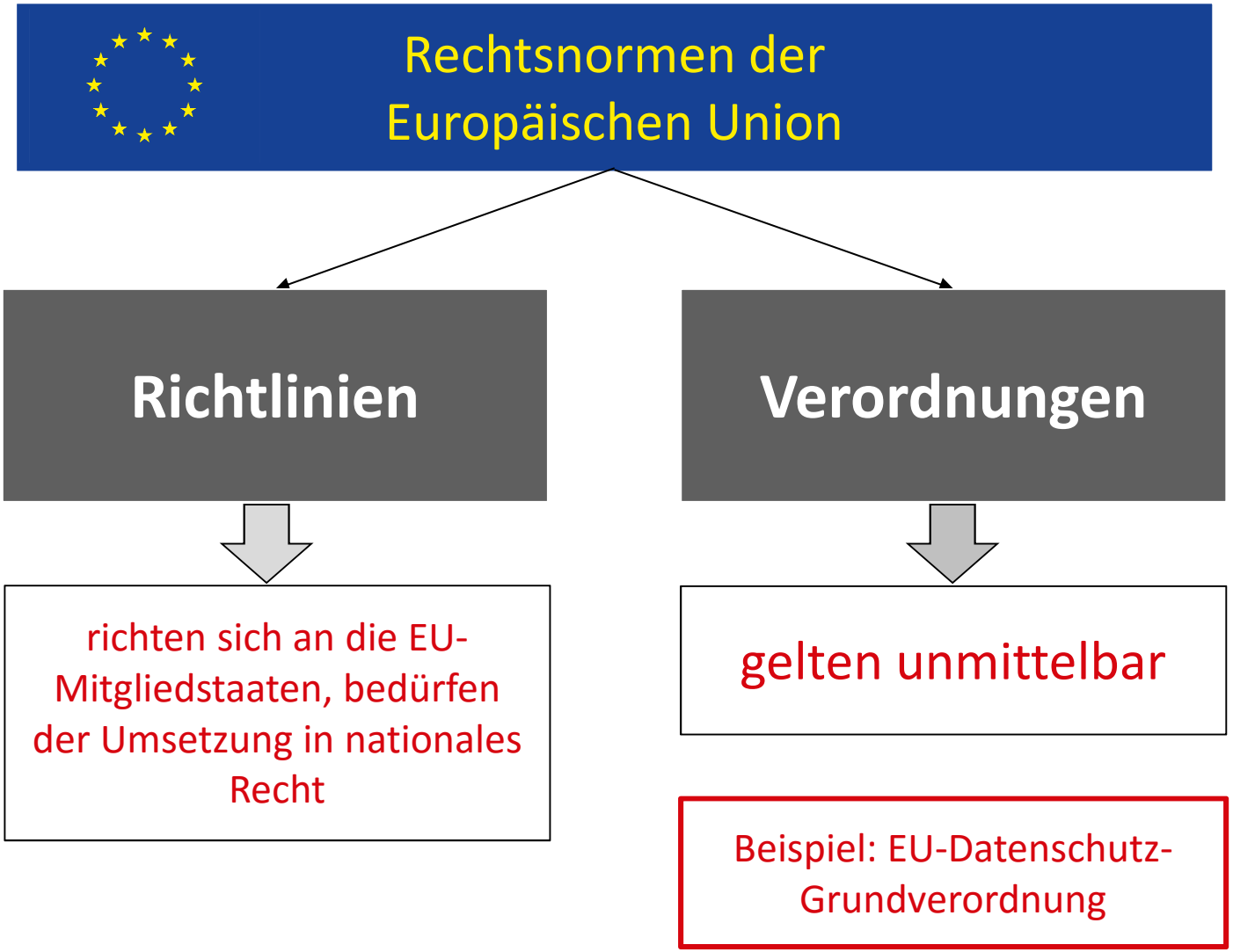
Unternehmergespräch am 16.05.2018

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

ZDF, 26.03.2018:

„Bundesjustizministerin Katharina Barley (SPD) setzt ihre Hoffnungen im **Facebook-Skandal** auf das neue europäische Datenschutzrecht. Danach werde man gegenüber einem Unternehmen wie Facebook Bußgelder in einer Höhe bis zu **1,6 Milliarden Euro** verhängen können, erklärte sie im ZDF. Barley bezog sich dabei auf die europäische Datenschutz-Grundverordnung, die am 25. Mai in Kraft tritt. Sie verschärft die Regeln für Unternehmen, die Daten sammeln. Bei Zuwiderhandlungen können Bußgelder verhängt werden, die bis zu **vier Prozent des weltweiten Jahresumsatzes** ausmachen.“

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE



HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

EU-Datenschutz-Grundverordnung (DS-GVO)

- vom 27.04.2016
- Fundstelle: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
- gilt ab dem **25. Mai 2018** (Art. 99 Abs. 2)
- gilt unmittelbar, enthält aber Öffnungsklauseln für nationales Recht:
- **Bundes-Datenschutzgesetz (BDSG) 2018**
- Fundstelle: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1522664341824
- Landesdatenschutzgesetze 2018 für die Landesbehörden

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Ziel: Schutz personenbezogener Daten, als Grundrecht

Definition „personenbezogene Daten“ (Art. 4 Nr. 1 DS-GVO):

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

„Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu einem Standort, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, psychologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werde kann.“

Beispiele: Name, Anschrift, E-Mail-Adresse, Geburtsdatum, Gesundheitsdaten, Bankdaten

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

DS-GVO: Was hat ein Unternehmen zu beachten?

- Interne **Zuständigkeit** klären
- Klären: Ist ein **Datenschutzbeauftragter** erforderlich?
- Prüfen: begründet Datenverarbeitung hohes **Risiko**, betrifft sensible Daten, ist durch Masse oder Relevanz kritisch?
- Überarbeiten der **Einwilligungserklärungen** bzw. **Verträge** (Kunden, Vertragspartner, Mitarbeiter)
- abschließen DS-GVO-konformer **Auftragsdatenverarbeitungsvereinbarungen**
- **Datenschutz** im Unternehmen intern **umsetzen**
- **Mustermeldungen und Meldeprozesse** vorbereiten

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Interne Zuständigkeit

- Geschäftsführung / Vorstand?
- Recht?
- Technik?
- Externe Beratung erforderlich?
- Budget vorhanden?

Vorgehensweise

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Erste Phase: **Reifegrad Analyse**	Zweite Phase: **Konzeption/ Planung der Umsetzung**	Dritte Phase: **Umsetzung**
Festlegung der zu prüfenden Unternehmensbereiche und des Umfangs der Prüfung.	Bewertung und Priorisierung des Anpassungsbedarfs und der notwendigen Maßnahmen	Konkrete Umsetzung der Maßnahmen gemäß Phase 2
Identifikation und Konkretisierung der Workstreams	Konkretisierung und Festlegung der Maßnahmen/Anpassungen	Abgleich/Update mit weiteren Konkretisierungen durch Aufsichtsbehörden/ Gesetzgeber
Skizzierung der Vorgehensweise und Durchführung einer ersten Reifegrad-Analyse und Einschätzung Aufwand	Abgleich/Update mit weiteren Konkretisierungen durch Aufsichtsbehörden/Gesetzgeber	

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Datenschutzbeauftragter

- Geregelt in Art. 37-39 DS-GVO, §§ 38, 5-7 BDSG
- Nichtöffentliche Stellen sind zur Benennung eines Datenschutzbeauftragten verpflichtet, wenn
  - in der Regel mehr als **10 Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder
  - Verarbeitungen vorgenommen werden, die einer **Datenschutz-Folgeabschätzung** unterliegen oder
  - personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Datenschutzbeauftragter

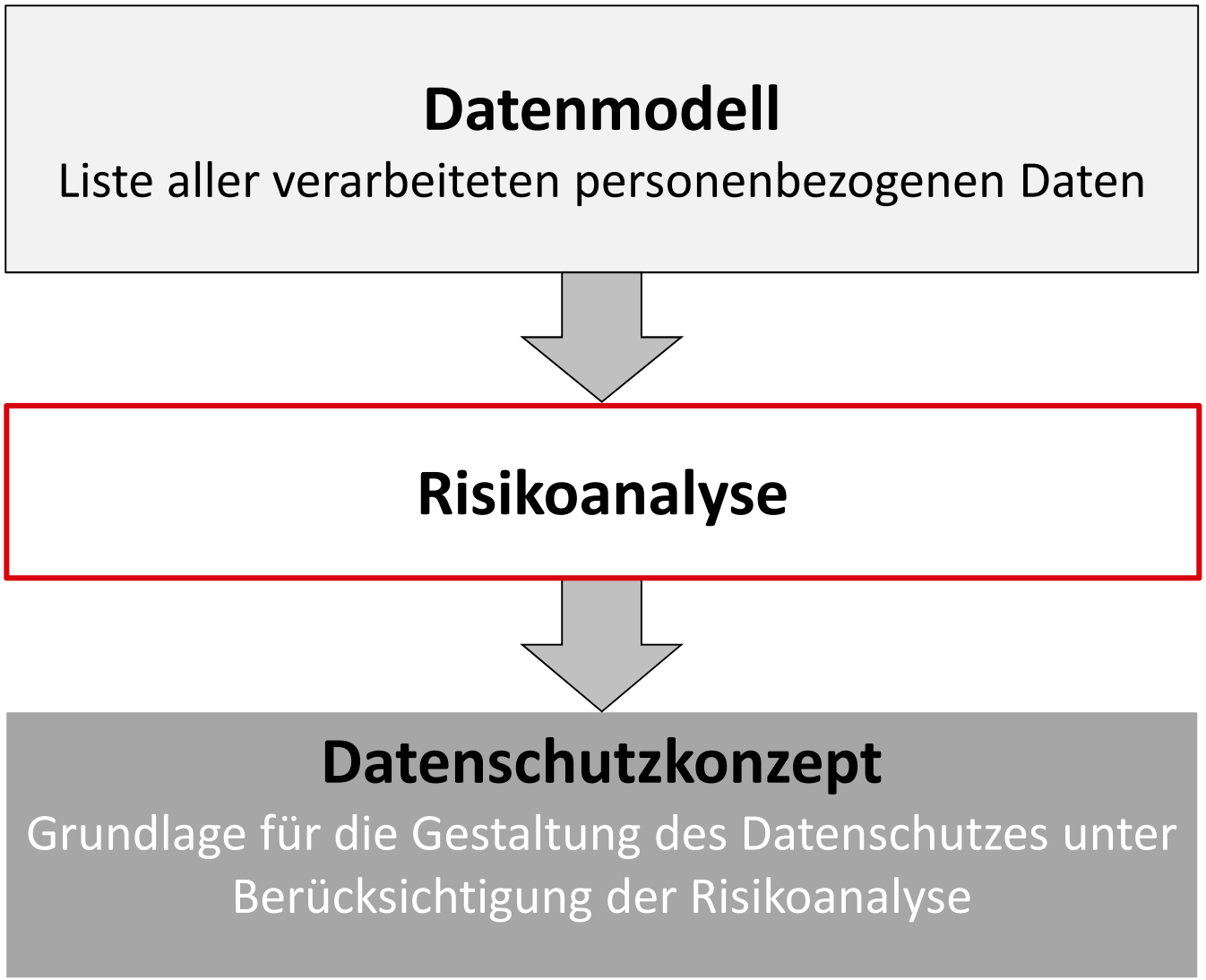
- Datenschutzbeauftragter:
  - intern: Arbeitnehmer, kein Geschäftsführer / Gesellschafter
  - extern: Dienstleister
- weisungsunabhängig, Art. 37 Abs. 3 DS-GVO
- Kündigungsschutz: § 6 Abs. 4 BDSG, Art. 37 Abs. 3 DS-GVO

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Datenschutzbeauftragter: Aufgaben (Art. 39 DS-GVO)

- **Unterrichtung und Beratung** hinsichtlich der Pflichten bezüglich des Datenschutzes
- **Überwachung** der Einhaltung des Datenschutzes, der Strategien zum Datenschutz einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter
- Auf Anfrage: Beratung im Zusammenhang mit der **Datenschutz-Folgeabschätzung**
- Zusammenarbeit mit der **Aufsichtsbehörde**
- **Anlaufstelle** für die Aufsichtsbehörde

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE



HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Risikoanalyse

- **Besteht ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen?
- **Indizien für hohes Risiko:**
  - Besonders schutzbedürftige Daten
  - Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen
  - Großer Umfang der Datensammlung
- **Risikokategorien:** normal – hoch – sehr hoch

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Hohes Risiko der Datenverarbeitung für die Rechte und Freiheiten von natürlichen Personen

- **Wenn ja:** Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung
- Regelung: Art. 35 DS-GVO, § 67 BDSG
- Erforderlich insbesondere bei:
  - systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen (Profiling)
  - umfangreiche Verarbeitung **besonderer Kategorien** von personenbezogenen Daten
  - systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Hohes Risiko: besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO)

- „Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“
- Gesundheitsdaten: „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person … beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“
- Beispiel: **Wettkampfergebnisse = Gesundheitsdaten?**
- **Positiv- oder Negativliste der Aufsichtsbehörde** nach Art. 35 Abs. 4 DS-GVO

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Datenschutz-Folgenabschätzung: Inhalt (Art. 35 Abs. 7 DS-GVO)

- **Systematische Beschreibung** der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen
- **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck
- **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen
- Zur Bewältigung der Risiken geplante **Abwehrmaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Datenschutz sichergestellt und der Nachweis dafür erbracht wird, dass die DS-GVO eingehalten wird

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)

- Von jedem Verantwortlichen zu führen
- Ausnahme: Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern, wobei Teilzeitbeschäftigte und Personen, die nicht das ganze Jahr beschäftigt sind, nur anteilig zählen und keine der nachbenannten Rückausnahmen greift:
  - die Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
  - die Datenverarbeitung nur gelegentlich erfolgt und
  - die Datenverarbeitung nicht die Verarbeitung besonderer Datenkategorien gemäß Art. 9 DS-GVO (insb. Gesundheitsdaten) einschließt
- Verzeichnis ist schriftlich oder elektronisch zu führen
- Das Verzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)

- Inhalt:
  - Kontaktdaten des Verantwortlichen, des Vertreters und des Datenschutzbeauftragten
  - Zwecke der Verarbeitung
  - Kategorien betroffener Personen und Kategorien personenbezogener Daten
  - Kategorien von Empfängern, gegenüber denen die Daten offengelegt werden
  - Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation
  - Wenn möglich: vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
  - Wenn möglich: allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen (TOM)** zum Datenschutz

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Einwilligungserklärungen / Verträge

- Einzuholen von:
  - Kunden
  - Teilnehmern an Sportveranstaltungen
  - Mitarbeitern
- kein Bestandsschutz für bisherige Einwilligungserklärungen
- schriftlich, mündlich oder elektronisch
- nicht: vorangekreuztes Kästchen
- ein Zweck = eine Einwilligung
- also: **bei jedem Neuabschluss / neuer Datenerfassung neue vertragliche Zustimmung bzw. vertragliche Zustimmung**

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Einwilligungserklärungen: Art. 7 DS-GVO

- Verantwortlicher muss Einwilligung / Vertrag nachweisen
- Einwilligung muss klar von anderen Sachverhalten zu unterscheiden sein
- Einwilligung kann jederzeit widerrufen werden. Widerruf muss so einfach wie die Einwilligung sein. Anders: Vertrag
- Kinder / Jugendliche: erteilen ab 16 die Einwilligung selbst, vorher: Erziehungsberechtigte

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

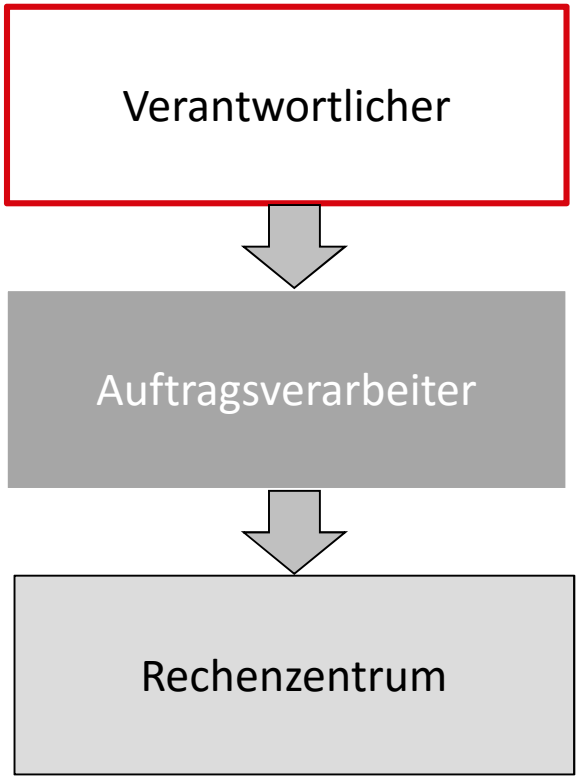
Datenschutzinformation: Art. 13, 14 DS-GVO

- in Verträgen / auf Websites
- Inhalt:
  - Namen und Kontaktdaten des Verantwortlichen
  - Kontaktdaten des Datenschutzbeauftragten
  - Zwecke der Datenverarbeitung (z. B. Kunden, Beschäftigte, Lieferanten)
  - bei Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen: Angabe der Interessen
  - Empfänger der Daten bei Datenübermittlung
  - Absicht, Daten in ein Drittland (außerhalb der EU) zu übermitteln
  - Löschfristen
  - Ansprüche der Berechtigten nach der DS-GVO (Auskunft, Berichtigung, Löschung, Sperrung, Widerspruch, Datenübertragbarkeit)
  - Recht des Betroffenen zum Widerruf einer Einwilligung
  - Recht des Betroffenen auf Beschwerde bei einer Datenschutzbehörde
- **Ausnahmen prüfen**

Auftragsverarbeitung (Art. 28 DS-GVO)

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

„Verarbeitung im Auftrag eines Verantwortlichen“



HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Auftragsverarbeitung (Art. 28 DS-GVO)

- Auftragsverarbeiter muss die hinreichende Garantie dafür bieten, das **geeignete TOMs** durchgeführt werden
- Inanspruchnahme weiterer Auftragsverarbeiter: nur mit vorheriger gesonderter oder allgemeiner Genehmigung des Verantwortlichen
- Bei allgemeiner schriftlicher Genehmigung zur Inanspruchnahme weiterer Auftragsverarbeiter:
  - Information über beabsichtigte Änderung
  - Verantwortlicher kann Einspruch erheben
- Erforderlich: **Vereinbarung zur Auftragsverarbeitung** mit gesetzlich bestimmtem Inhalt

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Auftragsverarbeitungsvereinbarung: Inhalt

- Datenverarbeitung nur auf Weisung des Verantwortlichen
- Gewährleistung der Verpflichtung des beteiligten Personals zur Vertraulichkeit
- Implementierung geeigneter TOMs
- Beachtung der Regelungen zur Einschaltung weiterer Auftragsverarbeiter
- Unterstützung durch geeignete TOMs bei der Wahrnehmung von Rechten betroffener Personen
- Unterstützung bei Meldepflichten
- Löschung oder Rückgabe der Daten nach Abschluss der Verarbeitungsleistung
- Ermöglichung von Überprüfungen durch den Verantwortlichen

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Auftragsverarbeitung: Fragen

- Auftragsverarbeitung außerhalb des Europäischen Wirtschaftsraums?

  Rechenzentrum im EWR-Ausland?

  Support aus dem EWR-Ausland?

  ⇨ Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DS-GVO zu dem betreffenden Land

- Vor-Ort-Kontrolle?

  Besuch im Rechenzentrum?

  ⇨ Ersetzung durch Zertifizierung oder sonstige Nachweise

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Datenschutz im Unternehmen

- Verantwortlicher muss Einhaltung des Datenschutzes **nachweisen** können (Art. 5 Abs. 2 DS-GVO)
- Einsetzung eines Datenschutzbeauftragten ist allein nicht ausreichend

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Maßnahmen zum Datenschutz im Unternehmen

- „Garantien“ = **Regelwerke, vertragliche Regelungen**
  - Standardvertragsklauseln
  - interne Datenschutzvorschriften
- **Privacy bei Design** (Art. 25 Abs. 1 DS-GVO): Datenschutz durch Technikgestaltung
  - TOMs zur Umsetzung der Datenschutzgrundsätze, z. B. Datenminimierung
  - z. B. Pseudonymisierung
- **Privacy bei Default** (Art. 25 Abs. 2 DS-GVO): Datenschutz durch datenschutzfreundliche Voreinstellungen
  - Verarbeitung nur solcher Daten, deren Verarbeitung für den Zweck erforderlich ist
  - gilt für Menge, Umfang, Speicherfrist und Zugänglichkeit
  - Schutz gegen Zugänglichkeit für unbestimmte Zahl von natürlichen Personen

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Vorbereitung von Prozessen für Meldungen

- Bei Verletzung des Schutzes personenbezogener Daten:
- **Meldung** an die Aufsichtsbehörde **binnen 72 Stunden**, nachdem die Verletzung bekannt wurde
- Ausnahme: keine Meldepflicht, wenn die Verletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt
- Inhalt der Meldung gesetzlich vorgegeben: Art. 33 Abs. 3 DS-GVO

⇨ **Meldeprozess ist zu implementieren**

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Vorbereitung von Prozessen für Meldungen

- Bei Verletzung des Schutzes personenbezogener Daten:
- **Benachrichtigung** der betreffenden Person **unverzüglich** (= ohne schuldhaftes Zögern)
- Ausnahmetatbestände (Art. 34 Abs. 3 DS-GVO) sind zu prüfen
- Aufsichtsbehörde kann ggf. Nachholung der Meldung fordern

⇨ **Meldeprozess ist zu implementieren**

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Vorbereitung zur Erfüllung von Auskunftsansprüchen

- Betroffene Personen haben einen Anspruch auf Auskunft
- Inhalt insbesondere:
  - Verarbeitungszwecke
  - Kategorien der verarbeiteten personenbezogenen Daten
  - Empfänger, gegenüber denen personenbezogene Daten offengelegt werden
  - Dauer, für die personenbezogene Daten gespeichert werden
  - Bestehen eines Rechts auf Berichtigung oder Löschung
  - Bestehen eines Beschwerderechts bei der Aufsichtsbehörde

⇨ **Auskunftsprozess ist zu implementieren**

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Vorbereitung zur Erfüllung von Löschungsansprüchen

- Betroffene Personen haben einen Anspruch auf Löschung von Daten (Art. 17 DS-GVO)
  - wenn die Daten für den Zweck der Verarbeitung nicht mehr erforderlich sind
  - die Person ihre Einwilligung widerruft
- Wurden Daten öffentlich gemacht:

  Verantwortlicher trifft angemessene Maßnahmen, um Löschung umzusetzen

⇨ Löschungsprozess ist zu implementieren

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Vorbereitung zur Datenübertragbarkeit (sog. Portabilität)

- Direkte Übermittlung von Daten, die vom Betroffenen bereit gestellt wurden, an neuen Verantwortlichen, z.B. Wechsel des E-Mail Providers.
- Dies setzt eine automatisierte Verarbeitung auf Basis von Einwilligung oder Vertrag in einem strukturierten, gängigen und maschinenlesbaren Format, voraus.
- Eine Beeinträchtigung von Rechten Dritter muss dabei ausgeschlossen werden.

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Bußgelder: Art. 83 DS-GVO

- Bis zu **20 Mio. € oder 4 % des weltweiten Jahresumsatzes**, je nachdem, was höher ist:
  - Verstoß gegen Grundsätze der Datenverarbeitung
  - Verstoß gegen Rechte betroffener Personen
  - rechtswidrige Übermittlung an Empfänger in einem Drittland
  - Nichtbefolgung einer Anweisung der Aufsichtsbehörde
- Bis zu **10 Mio. € oder 2 % des weltweiten Jahresumsatzes**, je nachdem, was höher ist:

  Verstöße gegen diverse nachrangige Pflichten
- Behördenprivileg: § 43 Abs. 3 BDSG 2018, § 32 E-LDSG NRW

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Haftung und Schadensersatz: Art. 82 DS-GVO

- Betroffene Person hat wegen eines Verstoßes gegen den Datenschutz einen Schadensersatzanspruch
- gegen den Verantwortlichen und den Auftragsverarbeiter
- auch wegen des immateriellen Schadens (**Schmerzensgeld**)
- Verantwortlicher / Auftragsverarbeiter kann sich exkulpieren, trägt dafür aber die Beweislast (praktisch nur: höhere Gewalt)
- **Verbandsklagerecht!** (Art. 80 DS-GVO, § 2 UKlaG)

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Fazit

- Relativ wenige Änderungen an den materiellen Anforderungen an den Datenschutz
- Sehr hohe Bußgelder
- Deutlich verschärfte Haftung (wegen des Schmerzensgeldes) und Verbandsklagerecht
- **Datenschutz wird im Bewusstsein der Betroffenen und der Behörden eine deutlich größere Rolle spielen als bisher**

HECKER
WERNER
HIMMELREICH
RECHTSANWÄLTE

Herzlichen Dank für Ihre Aufmerksamkeit!

Dr. Norbert Reuber
Rechtsanwalt
Fachanwalt für Verwaltungsrecht

Daniela Mechelhoff
Rechtsanwältin
Fachanwältin für Verwaltungsrecht

HECKER WERNER HIMMELREICH
Rechtsanwälte Partnerschaft mbB
Sachsenring 69
50677 Köln

Telefon: +49 (0)2 21 / 92 08 1 – 147/159
Telefax: +49 (0)2 21 / 92 08 1 – 88147/88159
E-Mail: rb@hwhlaw.de, dm@hwhlaw.de
Internet: www.hwhlaw.de