„MIND YOUR TAX & LAW“

Vortragsreihe

zu aktuellen Entwicklungen im

Steuer- und Wirtschaftsrecht

Zeißstraße 63 • 30519 Hannover • Tel.: (0511) 920 600 28
post@askgruppe.de • www.askgruppe.de

Die Europäische Datenschutzgrundverordnung (DSGVO)

Neuer Datenschutz in der Praxis – Pflichten für Unternehmen

RA Wolfgang Stannek, Dipl.-Ök.

Disclaimer

1. Der Vortrag stellt keine juristische Beratung dar. Diese ist immer einzelfallabhängig.

2. Es werden nicht alle Inhalte der DSGVO dargestellt.

3. Bei Bedarf vermitteln wir gerne zwischen Ihnen und unseren Kooperationspartnern, die sich auf die operative Umsetzung datenschutzbezogener Inhalte spezialisiert haben. Für etwaige rechtliche Fragestellungen stehen wir bei Bedarf gerne als Ansprechpartner zur Verfügung.

Inhaltsübersicht

1. Warum Datenschutz?
2. Grundlagen und Begrifflichkeiten
3. Wesentliche Neuerungen und Pflichten im Überblick
4. Berührungspunkte im Unternehmen
5. Anforderungen aus Umsetzungssicht
6. Umsetzung im Unternehmen

Warum Datenschutz?

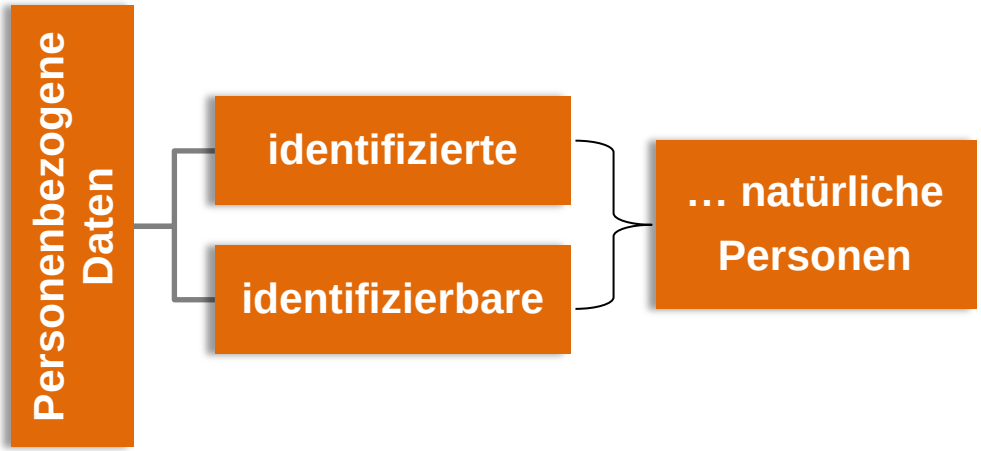
- ✓ **Allgemeines Persönlichkeitsrecht („APR“)**
  - **Setzt sich zusammen aus Art. 2 I GG (Recht auf freie Entfaltung) und Art. 1 I GG (Menschenwürde)**
- ✓ **Besondere Ausprägung des APR ist das Recht auf „informationelle Selbstbestimmung“**
  - **Jeder darf selbst über die Herausgabe und Verwendung seiner personenbezogenen Daten bestimmen**
  - **Zweck: Abwehr von Eingriffen des Staates in die Privatsphäre des Einzelnen**
    - ➢ **mittelbar wirkt sich das APR aber auch auf das Zivilrecht aus (P <-> P)**
  - **Die Bewahrung dieses Grundrechts soll der Datenschutz bewerkstelligen**

Was ist die DSGVO?

- ✓ Die EU-Datenschutz-Grundverordnung („DSGVO“) bereits seit 24.05.2016 in Kraft
- ✓ Unmittelbare Anwendung ab 25.05.2018
  - ➢ Unternehmen müssen ab diesem Datum sämtliche Dokumente u. Prozesse angepasst haben
- ✓ Vereinheitlicht die Regelungen zum Datenschutz in der gesamter EU
  - ➢ Schutz personenbezogener Daten
  - ➢ Trägt zu gleichen Wettbewerbsbedingungen bei
- ✓ In Deutschland galt bisher das Bundesdatenschutzgesetz (BDSG), welches die alte europäische Datenschutzrichtlinie umsetzt. Im Gegensatz dazu wird die DSGVO unmittelbar geltendes Recht (RL <-> VO).
- ✓ Bundesdatenschutzgesetz (BDSG - neu) gilt neben DSGVO weiter; DSGVO hat aber das „letzte Wort“, sofern keine „Öffnungsklausel“ für einzelstaatliche Regelung vorhanden

Personenbezogene Daten

- ✓ **Personenbezogene Daten** (vgl. Art. 4 Abs. 1 DSGVO)



- Name
- Geburtsdatum
- Kontaktdaten (Adresse, Telefonnummer etc.)
- Alter
- Geschlecht
- Kontodaten
- Vermögen
- Sozialversicherungs-nummer
- IP-Adresse
- Bewegungsdaten
- etc.

- ➢ Angaben, die sich einer bestimmten natürlichen Person (der **„Betroffenen“** = Menschen) zuordnen lassen und sie dadurch identifizieren oder identifizierbar machen kann.
  - **identifiziert** = Information → Auskunft über Identität
  - **identifizierbar** = Kombination von Informationen/Daten → Rückschluss auf Identität

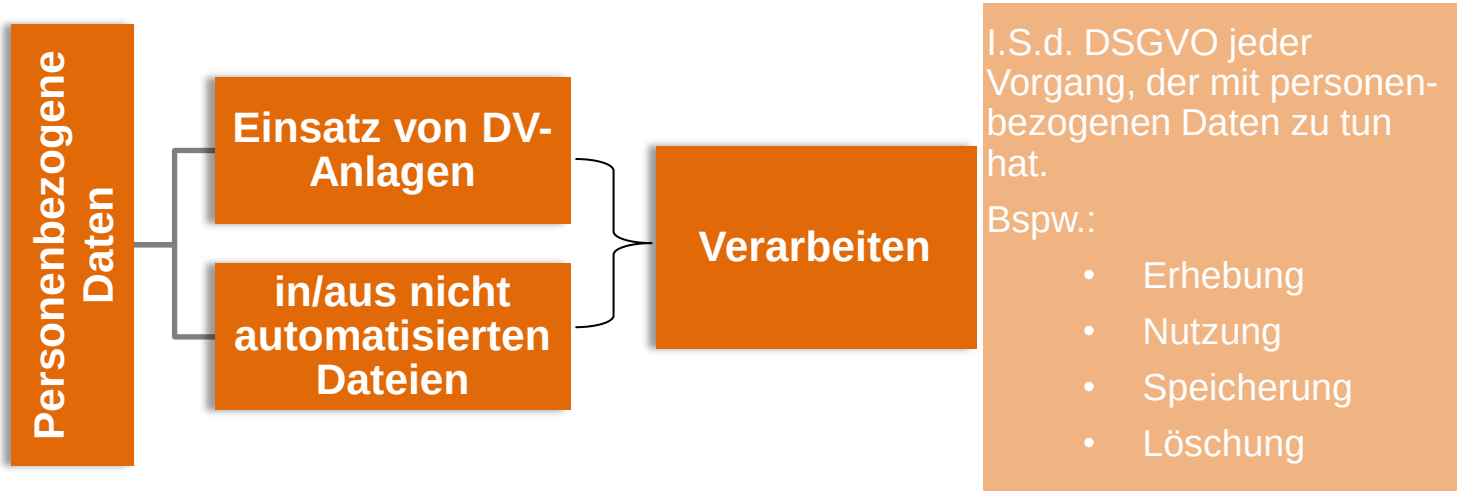
- Kunden
- Beschäftigte
- Lieferanten

Besondere Arten personenbezogener Daten

- ✓ **<u>Besondere Arten</u> personenbezogener Daten**
  - ➢ **sind in höherem Maße sensibel und unterliegen einem verschärften Schutz.**
- ✓ **In diese Kategorie fallen Angaben zu:**
  - rassischer und ethnischer Herkunft
  - politischen Meinungen
  - religiösen / weltanschaulichen Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Gesundheit und Sexualität
  - ➢ **Diese Daten dürfen nur mit ausdrücklicher Einwilligung der betroffenen Person verarbeitet werden.**

Anwendungsbereich der DSGVO

- ✓ **DSGVO gilt für Unternehmen, aller Branchen innerhalb der EU, die:**



- ✓ **Unternehmen außerhalb der EU, wenn sie:**
  - **eine Niederlassung in der EU haben oder**
  - **personenbezogene Daten von EU-Bürgern verarbeiten**

Ausgenommen: Erhebung, Verarbeitung und Nutzung personenbezogener Daten für ausschließlich persönlich oder familiäre Zwecke und Tätigkeiten (Adressbücher, Fotos etc.)

Verbot mit Erlaubnisvorbehalt

- ✓ **Allgemeiner Grundsatz für die Verarbeitung personenbezogener Daten:**

„Verbot mit Erlaubnisvorbehalt“

„Es ist grundsätzlich verboten,

was nicht ausdrücklich erlaubt ist.“

- ➢ **Konkret: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten – es sei denn, es liegt eine ausdrückliche Erlaubnis vor.**
- ➢ **Diese kann in folgenden zwei Formen vorliegen:**
  - **Rechtsgrundlage erlaubt/ordnet Verarbeitung an oder**
  - **es liegt eine Einwilligung des Betroffenen vor**

Wesentliche Neuerungen und Pflichten für Unternehmen

Sanktionen

Geldbußen:
bis zu 20 Mio. EUR oder bis zu 4 % des gesamten weltweiten Jahresumsatzes

Meldepflicht

Bei Datenschutzverletzung (z.B. Datenpanne)
→ Meldung innerhalb von 72 Stunden;
→ Pflicht entfällt, wenn Verletzung „voraussichtlich nicht zu Risiko für Rechte und Freiheiten natürlicher Personen führt“ (Art. 33 DSGVO)

Betroffenenrechte

- z.B. Recht auf:
- (kostenfreie) Auskunft
- Löschung
- Sperrung
- Berichtigung
- Widerspruch
- Schadensersatz

Privacy by design & Privacy by default

„by design“

Technische u. organisatorische Maßnahmen (TOMs) zum Schutz personenbez. Daten sollen bereits bei der Entwicklung von Vorgängen mit einbezogen werden → Datenschutz als Standard

„by default“

Voreinstellungen sollen bereits datenschutzfreundlich sein, sodass personenbez. Daten ohne besondere Anpassungen von vornherein geschützt sind

Verfahrensverzeichnis

Datenschutzorganisation

ggf. Benennung eines Datenschutzbeauftragten und Aufbau einer DSGVO kompatiblen „Datenschutzorganisation Verarbeitungsaktivitäten“

Datenschutz-Folgenabschätzung

Vor Beginn der DV vorzunehmen und zu dokumentieren.
Pflicht insbesondere dann, wenn die DV voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat

Berührungspunkte im Unternehmen

- ✓ Speicherung und Verarbeitung Mitarbeiterdaten
- ✓ Kunden- und Lieferantendaten
- ✓ Kontakt und Adressdaten
- ✓ Auftragsverarbeitung (AV)
  - IT-Wartung
  - Nutzung von Cloud-Diensten (Auslagerung von Daten und Anwendungen)
  - externe Lohn- oder Gehaltsabrechnung
  - Datenträgerentsorgung
  - Versand eines Newsletters durch eine Agentur
- ✓ Webseiten-Kontaktformular ohne Einwilligung in Datenschutzbestimmungen
- ✓ Webseiten (Anpassung der Datenschutzerklärung)

Anforderungen an Unternehmen aus Umsetzungssicht (I)

- ✓ **Folgende Prozesse / Dokumente sollten Sie in ihrem Unternehmen prüfen bzw. vorhalten:**
  - **Dokumentation der Verarbeitung personenbezogener Daten in einem unternehmensweiten „Verzeichnis von Verarbeitungstätigkeiten“ (Art. 30 DSGVO)**
  - **Durchführung einer Datenschutz-Folgeabschätzung (Art. 35 DSGVO) → Privacy Impact Assessment („PIA“)**
  - **Einwilligungserklärungen (Umsetzung der Anforderungen der Artt. 7, 13 DSGVO - Verschärfung der formalen Vorgaben) → einzeln, aktiv, leicht verständlich und detailliert einzuholen; muss nachgewiesen werden**
  - **Prozess für den Widerruf von Einwilligung und Widersprüchen**
  - **Anpassungen der Datenschutzerklärung zur datenschutzkonformen Information der Betroffenen (Erweiterung der Informationspflichten, Artt. 13,14 DSGVO)**
  - **Prozess und Sicherstellung der weiteren Betroffenenrechte (Artt. 15-22 DSGVO - Auskunft, Berichtigung, Löschung, Portabilität etc.)**

Anforderungen an Unternehmen aus Umsetzungssicht (II)

- ✓ **Das ist noch nicht alles ...**
  - **Anpassung bestehender Verträge mit Auftrags(daten)verarbeitern (Art. 28 DSGVO) - d.h. mit Unternehmen, die im Auftrag Ihres Unternehmens personenbezogene Daten verarbeiten (z.B. Callcenter, ext. Lohnbuchhaltung, IT-Wartung), an die neuen Regelungen (Haftungsregelung, Dokumentation)**
  - **Prozess zur Meldung von Datenschutzverstößen (Accountability - deutlich erweiterte Nachweispflichten)**
  - **Risk Assessment – Ergreifung geeigneter „technischer und -organisatorischer Maßnahmen (TOMs) → Verschlüsselung, Stabilität, Widerherstellbarkeit u. regelmäßige Überprüfung**
  - **zielgruppengerechte Schulungen (Neuerungen der DSGVO und eigener Prozesse), Fortbildungen und Monitoring der nationalen Gesetzgebung**

Hinweis:

Effektives Datenschutzmanagementsystem (DMS) mit den oben aufgeführten Prozessen kombinieren/integrieren und Einzelschritte dokumentieren.

- ➢ **Nachweis ggü. Aufsichtsbehörde, dass geeignete Strategien erarbeitet und Maßnahmen ergriffen wurden.**

Umsetzung im Unternehmen

1. Bestandsaufnahme
(IST-Analyse)

- Betroffenheitsanalyse
- Bestandsaufnahme:
  - ➢ rechtlich
  - ➢ technisch
  - ➢ organisatorisch

z.B.:
- Prozesse, in denen personenbez. Daten verarbeitet werden
- dazugehörige RGL
- Datenschutzorganisation (Maßnahmen zum Schutz personenbez. Daten)
- Dienstleistungsbeziehungen
- Dokumentation (VerVerz, IT-Sicherheitskonzepte etc.)

2. Handlungsbedarf ermitteln
(Gap-Analyse)

- SOLL-IST-Abgleich

z.B.:
- Verzeichnis von Verarbeitungstätigkeiten
- RGL
- Betroffenenrechte
- Dokumentationspflichten (VerfVerz)
- Datenschutz-Folgenabschätzung
- Meldepflichten (DS-Beauftragter), Verletzungen)
- Datensicherheit (Zugriffsrechte, Viren, Hacker etc.)

➢ **Maßnahmenplan**

3. Umsetzung

z.B.:
- ggf. Bestellung eine DSB
- Anpassung der Datenschutz-organisation (Datenschutz-konzept/-richtlinie)
- Verpflichtung der MA auf Datengeheimnis
- Einrichtung von TOMs zur Gewährleistung der Daten-sicherheit
- Implementierung von Löschkonzepten
- Reaktionsmechanismen bei Datenpannen

➢ **Datenschutzmanagement-system (DMS)**

Herzlichen Dank!

E-Mail: post@askgruppe.de