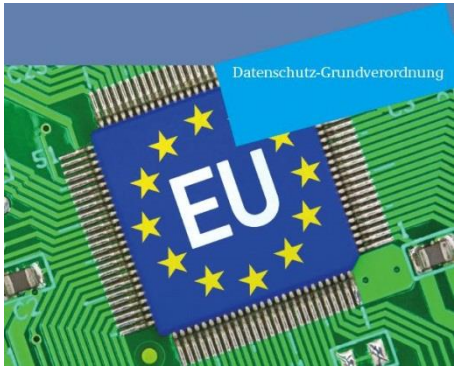
Datenschutzgrundverordnung

-

Ein Leitfaden zur Rechtssicherheit



Dr. Thorsten Hauröder, Rechtsanwalt
Bahar Beyaz, Rechtsanwältin

08.05.2018

Inhalt

I. Einleitung

1. Änderung des Datenschutzrechtes ab dem 25.05.2018
2. Anwendungsbereich der DSGVO
3. Begriffsbestimmungen
4. Verarbeitung von personenbezogenen Daten nach der DSGVO

1. Änderung des Datenschutzrechtes ab dem 25.05.2018

- Datenschutzgrundverordnung (DSGVO)
- Datenschutz-Anpassungs und Umsetzungsgesetz EU- DSAnpUG-EU (BDSGneu)
- E-Privacy-Verordnung (voraussichtlich erst ab 2020)

Henseler & Partner RECHTSANWÄLTE mbB

2. Anwendungsbereich der DSGVO

Sachlicher Anwendungsbereich, Art. 2 DSGVO

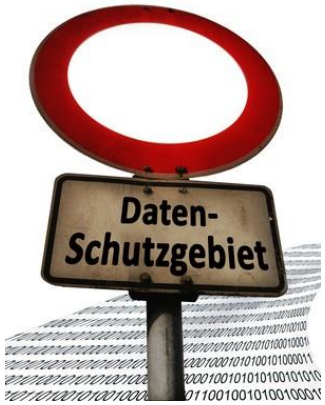
- Ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten
- Nichtautomatisierte Datenverarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind
  oder gespeichert werden sollen

Persönlicher Anwendungsbereich, Art. 3 I DSGVO

- Verarbeitung personenbezogener Daten durch Verantwortliche und durch Auftragsverarbeiter

Räumlicher Anwendungsbereich, Art. 3 II u. III DSGVO

- Verarbeitung durch Verantwortlichen mit Sitz in der EU – unabhängig davon, ob die Verarbeitung selbst in der Union stattfindet
- Verarbeitung personenbezogener Daten von sich in der Union befindenden Betroffenen durch einen nicht in der Union niedergelassenen Verantwortlichen, wenn diese Verarbeitung im Zusammenhang steht
  den Betroffenen in der Union Waren/Dienstleistungen anzubieten
  das in der Union erfolgende Verhalten Betroffener zu beobachten
  (Marktortprinzip)



Henseler & Partner RECHTSANWÄLTE mbB

3. Begriffsbestimmungen, Art. 4 DSGVO

- **Personenbezogene Daten, Art. 4 Nr. 1 DSGVO**
  - Alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen
  - Beispiel: Name, E-Mailadresse, IP-Adresse, Fotos

- **Verarbeitung, Art. 4 Nr. 2 DSGVO**
  - Jeder Vorgang zur Erhebung, Erfassung, Organisation, Speicherung, Veränderung, Abfrage, Bereitstellung, Verknüpfung oder sonstigen Verwendung einschließlich die Löschung oder Vernichtung von Daten
  - Beispiel: Speicherung von Kunden- und Beschäftigtendaten, Weitergabe an Dritte

- **Verantwortlicher, Art. 4 Nr. 7, Art. 24 DSGVO**
  - Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

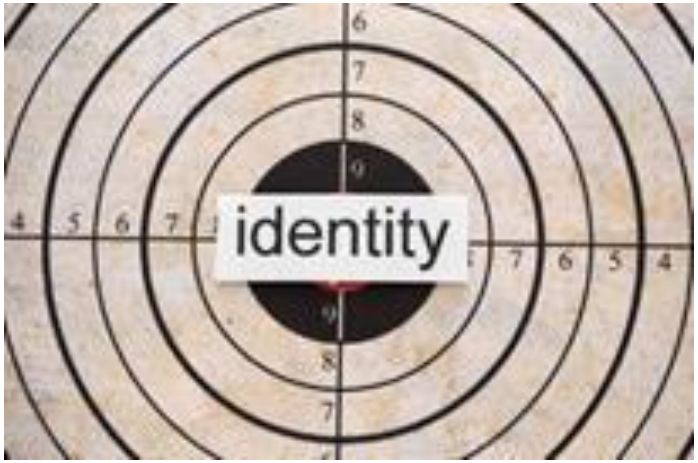
- **Auftragsverarbeiter, Art. 4 Nr. 8 DSGVO, Art. 28 DSGVO**
  - Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
  - Beispiel: Lohnbuchhaltung, Aktenvernichtungsunternehmen

- **Betroffene Person**
  - Subjekt der Datenverarbeitung

4. Verarbeitung von personenbezogenen Daten nach der DSGVO

➢ Grundsätze der Verarbeitung, Art. 5 DSGVO

- Rechtmäßigkeit
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität/Vertraulichkeit
- Rechenschaftspflicht/Dokumentation



4. Verarbeitung von personenbezogenen Daten nach der DSGVO

➢ Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der genannten nachstehenden Bedingungen erfüllt ist. Ansonsten ist sie verboten (Verbotsprinzip mit Erlaubnisvorbehalt).

- Einwilligung, Art. 6 I a DSGVO
- Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person, Art. 6 I b DSGVO
- Erfüllung einer rechtlichen Verpflichtung, Art. 6 I c DSGVO
- Zum Schutz lebenswichtiger Interessen, Art. 6 I d DSGVO
- Wahrnehmung einer Aufgabe im öffentlichen Interesse, Art. 6 I e DSGVO
- Wahrnehmung der berechtigten Interessen des Verantwortlichen oder eines Dritten / Interessen der betroffenen Person stehen nicht entgegen, Art. 6 I f DSGVO
  → Interessenabwägung

II. Pflichten von Unternehmen

(Abweichende Vorgaben für öffentliche Stellen)

1. Bestellung eines Datenschutzbeauftragten
2. Bereitstellung einer Datenschutzerklärung/Informationspflichten
3. Auftragsdatenverarbeitungsverträge
4. Überprüfung der Ermächtigungsgrundlage für die Verarbeitung und die Weitergabe von personenbezogener Daten
5. Überprüfung Einwilligungen
6. Anlegen von Verarbeitungsverzeichnissen
7. Schaffung von technischen und organisatorischen Maßnahmen
8. Datenschutzfolgenabschätzung
9. Erstellen von Löschkonzepten
10. Notfallplan bei Datenverlust/Meldepflicht

1. Bestellung eines Datenschutzbeauftragten, Art. 37 ff. DSGVO

- **Bestellpflicht, wenn mindestens zehn Personen sich ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind**
- **Bestellpflicht auch unabhängig von der Anzahl der Mitarbeiter auch dann, wenn Verarbeitungen einer Datenschutzfolgenabschätzung unterliegen oder die Verarbeitung zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung erfolgt**
- **Bestellpflicht außerdem auch dann, sofern umfangreiche, regelmäßige und systematische Überwachung stattfindet oder die umfangreiche Verarbeitung besonderer Kategorien von Daten (Art. 9 und 10) erfolgt**
- **Externe oder interne Bestellung möglich**
- **Personelle Anforderungen**
  - Fachwissen entsprechend Niveau durchgeführter Datenverarbeitungsvorgänge und entsprechend Schutzbedürftigkeit personenbezogener Daten

1. Bestellung eines Datenschutzbeauftragten, Art. 37 ff. DSGVO

- **Pflichten, Art. 39 Abs. 1 DSGVO**
  - Geheimhaltung und Vertraulichkeit
  - Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen über datenschutzrechtliche Pflichten
  - Überwachung der Einhaltung der DSGVO sowie anderer Datenschutzvorschriften
  - Überwachung der Strategien des Verantwortlichen und Auftragsverarbeiters für den Schutz personenbezogener Daten
  - Beratung – auf Anfrage – im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung ihrer Durchführung
  - Anlaufstelle für und Zusammenarbeit mit der Aufsichtsbehörde

- **Haftung des Datenschutzbeauftragten**
- **Meldepflicht bei der Aufsichtsbehörde bis zum 25.05.2018!**

2. Bereitstellung einer Datenschutzerklärung/Informationspflichten

- **Pflicht zur Bereitstellung einer Datenschutzerklärung**
- **Informationspflichten nach Art. 13 und 14 DSGVO**
- **Inhalt einer Datenschutzerklärung**
  - Kontaktdaten des Verantwortlichen
  - die Zwecke und die Rechtsgrundlage der Verarbeitung der personenbezogenen Daten
  - Speicherdauer
  - die Rechte der Betroffenen
  - die ggfs. geplante Übermittlung der personenbezogenen Daten an Drittländer
  - die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
  - die Kontaktdaten des Datenschutzbeauftragten

3. Auftragsdatenverarbeitungsverträge, Art 28 DSGVO

- **Auftragsverarbeitung: Verarbeitung von Daten im Auftrag und auf Weisung des Verantwortlichen**
- **Abzugrenzen von der Funktionsübertragung**
- **Beispiele: Lohnbuchhaltung, Aktenvernichtung, IT-Unternehmen, Unternehmen die CRM-Systeme zur Verfügung stellen**
- **Inhaltliche Anforderungen an Auftragsdatenverarbeitugngsvertrag**
  - Gegenstand und Dauer der Verarbeitung
  - Art und Zweck der Verarbeitung
  - Die Art der personenbezogenen Daten
  - Die Kategorien betroffener Personen
  - Pflichten und Rechte des Verantwortlichen

4. Überprüfung der Ermächtigungsgrundlagen für die Verarbeitung und die Weitergabe von personenbezogenen Daten

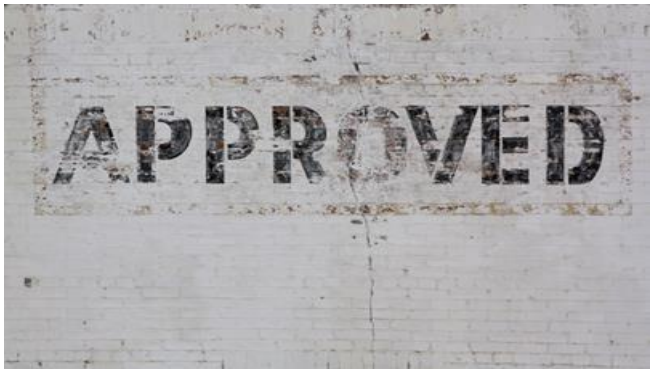
- **Bestandsaufnahme**
  - Welche personenbezogenen Daten werden verarbeitet?
  - Auf welcher Ermächtigungsgrundlage werden diese verarbeitet?
  - Erfolgt eine Weitergabe von personenbezogenen Daten an Dritte?
  - Auf welcher Ermächtigungsgrundlage beruht die Weitergabe?

- **Ermächtigungsgrundlage**
  - Einwilligung
  - Gesetzliche Grundlage (Art. 6 DSGVO)
  - Auftragsdatenverarbeitungsvertrag bzw. Unterauftragsdatenverarbeitungsvertrag

- **Übermittlung in Drittländer**
  1. Stufe: Ermächtigungsgrundlage
  2. Stufe: Angemessenes Datenschutzniveau im Drittland

5. Überprüfung von Einwilligungen, Art. 7 DSGVO

- **Schriftlich, mündlich oder elektronisch möglich**
- **Verständliche und leicht zugängliche Form in klarer und einfacher Sprache**
- **Eindeutige Abgrenzung von Sachverhalten, Einzelfallbezug**
- **Angabe von Zwecken**
- **Jederzeitige Widerruflichkeit**
- **Hinweis auf Widerruflichkeit, Art. 21 Abs. 4 DSGVO**
- **Freiwilligkeit**
- **Koppelungsverbot**
- **Dokumentation**



6. Anlegen von Verarbeitungsverzeichnissen, Art. 30 DSGVO

- **Grundsätzlich verpflichtend für jeden Verantwortlichen und jeden Auftragsverarbeiter**
- **Ausnahme: nicht verpflichtend für Unternehmen mit weniger als 250 Mitarbeitern**
  - sofern kein Risiko für die Rechte und Freiheiten der Betroffenen durch die Datenverarbeitung besteht oder
  - sofern die Datenverarbeitung nicht nur gelegentlich erfolgt oder
  - sofern keine besonderen Arten personenbezogener Daten betroffen sind (Art. 9 und Art. 10 DSGVO)
- **Form: schriftlich oder elektronisch**
- **Zuständig für die Durchführung: Unternehmensleitung, nicht Datenschutzbeauftragter**
- **Inhalt der Angaben durch den Verantwortlichen (Art. 30 Abs. 1 DGSVO)**
  - Name und Kontaktdaten; Zweck der Verarbeitung; Kategorien betroffener Personen und Personenbezogener Daten; Kategorien von Datenempfängern; Übermittlungen in Drittländer; Löschfristen; Angaben zur Datensicherheit
- **Inhalt der Angaben durch den Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO)**
  - Name und Kontaktdaten; Kategorien von Verarbeitungen; Übermittlung in Drittländer; Angaben zur Datensicherheit

7. Schaffung von technischen und organisatorischen Maßnahmen, Art. 32 DSGVO

- **Einführung eines angemessenen Sicherheitsstandards**
- **Zweck: Gewährleistung von Datensicherheit**
- **Indizwirkung durch Einhaltung von Verhaltensregeln (Art. 40 DGSVO) und genehmigten Zertifizierungsverfahren (Art. 42 DSGVO)**
- **Technische Maßnahmen**
  - Einhaltung des „Standes der Technik“
  - Verschlüsselung personenbezogener Daten (Bsp. SSL-Verbindung Webseite)
  - Pseudonomysierung personenbezogener Daten
  - Einrichtung technischer Zugriffskontrollen
- **Organisatorische Maßnahmen**
  - Beaufsichtigung von Personal, das Zugang zu personenbezogenen Daten hat
  - Einrichtung physischer Zutritts-, Zugriffs- oder Zugangskontrollen
  - Für die Wiederherstellung von Daten: Personalplanung und Notstromversorgung
  - Minimierung der Verarbeitung personenbezogener Daten
  - Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen

8. Datenschutzfolgenabschätzung, Art. 35 DSGVO

- **Verpflichtend für Verantwortliche, nicht Auftragsverarbeiter oder Datenschutzbeauftragte**
- **Bestehen eines voraussichtlich hohen Risikos für die persönlichen Rechte und Freiheiten von betroffenen Personen**
- **Bewertung der Eintrittswahrscheinlichkeit und Schwere des möglichen Risikos**
- **Bewertung der Art, des Umfangs, der Umstände, der verfolgten Zwecke sowie Ursachen möglicher Risiken für Rechte und Freiheiten der betroffenen Personen**
- **Überprüfung von Maßnahmen, Garantien und Verfahren, um bestehende Risiken einzudämmen**
- **Indizien für Erforderlichkeit:**
  - Neue Technologien
  - Neue Verarbeitungen
  - Verarbeitung großer Datenmengen
  - Sensibilität
  - Profiling
  - Öffentliche Überwachung, Bsp. Videoüberwachung

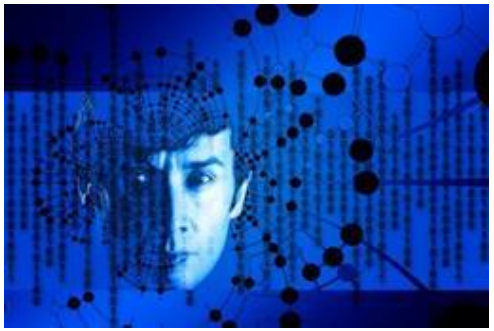
9. Erstellen von Löschkonzepten

- **Grundsatz der Datenminimierung nach Art. 5 DSGVO**
- **Definition von klaren Regeln und Zuweisung von nachvollziehbaren Verantwortlichkeiten**
- **Zu berücksichtigende Aspekte:**
  - Nach Datenarten kategorisierte Vorhaltefristen
  - Technische Anforderungen an die Löschung bestimmter Daten
  - Verantwortlichkeiten für die Freigabe von Regellöschfristen
  - Verantwortlichkeiten für Durchführung der Löschung
  - Kontrolle und Durchsetzung der Datenlöschung

10. Notfallplan bei Datenverlust/Meldepflicht, Art. 33 und 34 DSGVO

- **Meldepflicht für den Verantwortlichen**
- **Pflicht des Auftragsverarbeiters Datenschutzverletzung unverzüglich dem Verantwortlichen zu melden**
  - Gegeben bei Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung/Zugang
  - Grund sowie Vorsatz oder Fahrlässigkeit unerheblich
- **Grundsatz: Unverzügliche Meldepflicht bei der Aufsichtsbehörde innerhalb von 72 Stunden bei Datenschutzverletzung**
- **Ausnahmsweise keine Meldepflicht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führt**
- **Meldepflicht auch gegenüber der betroffenen Person, sofern voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht**

III. Rechte der Betroffenen



1. Recht auf Widerruf, Art. 7 DSGVO
2. Recht auf Auskunft, Art. 15 DSGVO
3. Recht auf Bestätigung, Art. 15 DSGVO
4. Recht auf Erhalt einer Kopie, Art. 15 Abs. 3 DSGVO
5. Recht auf Berichtigung, Art. 16 DSGVO
6. Recht auf Löschung, Art. 17 DSGVO
7. Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO
8. Recht auf Datenübertragbarkeit, Art. 20 DSGVO
9. Recht auf Widerspruch, Art. 21 DGSVO
10. Recht auf Beschwerde bei der Aufsichtsbehörde, Art. 77 DSGVO

IV. Fazit & Ausblick

- **Offene Rechts- und Anwendungsfragen**
- **Spielräume für nationale Aufsichtsbehörden durch Öffnungsklauseln**
- **Ahndung und Verhängung von Bußgeldern durch Aufsichtsbehörden**
- **Zeitdauer für gefestigte EU-Rechtsprechung**

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Thorsten Hauröder – Thauroeder@hp-legal.com
Bahar Beyaz – Bbeyaz@hp-legal.com