Neuerungen DSGVO

ab 25. Mai 2018

- 24.05.2016 Inkrafttreten DSGVO, Beginn der Umsetzungsfrist in EU
- **25.05.2018 Geltung der DSGVO**

DSG 2000 → DSG 2018 (inkl. DSDRG)

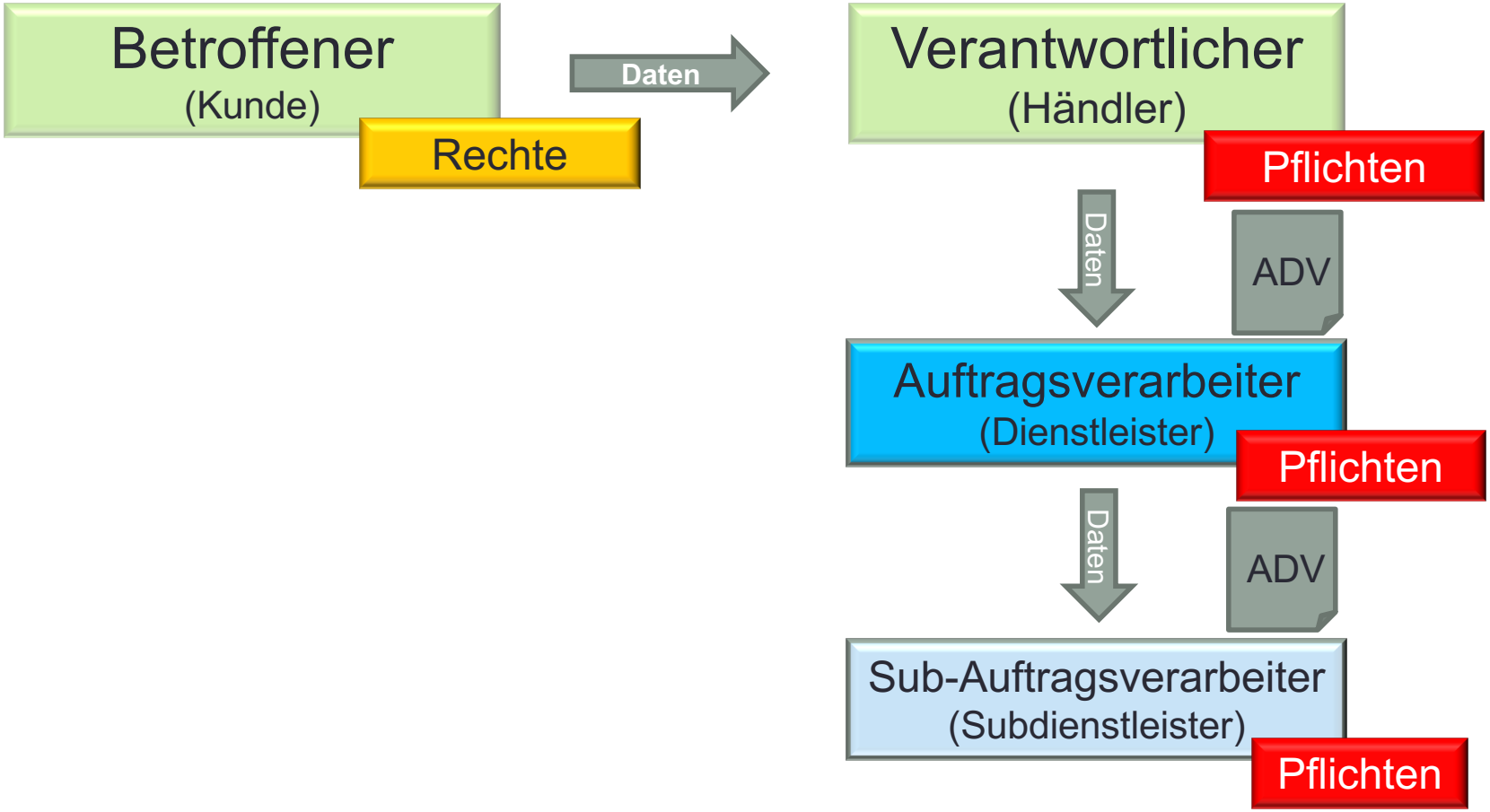
- Gesetz gilt für Unternehmen **jeder Größenordnung**
- **Marktortprinzip** - wer im Rahmen unternehmerischer Tätigkeit Personendaten verarbeitet: Niederlassung oder Kunden in der EU
- **Datenschutzbehörde (DSB)** - DVR entfällt
- **Pflichten** der Verantwortlichen
- **Rechte** der Betroffenen
- **Meldepflichten** DataBreach an Betroffene & DSB
- **Dokumentationspflicht** für Unternehmen
- **Rechtsgrundlagen** - Verwendungs-Zustimmung
- **Technikgestaltung** + **Datensicherungsmaßnahmen (TOM)**
- auch bei systematischer **nicht-elektronischer** Datenverarbeitung
- Ausnahmen für einzeln Bestimmungen (z.B. Datenschutzfolgenabschätzung)

→ Mehr Eigenverantwortung

Strafen & Auswirkungen

- bis zu 20 Mio € oder 4% des weltweiten Jahresumsatzes
  - Verletzung der Prinzipien inkl. der Bedingungen für Einwilligungen
  - Verletzung der Betroffenenrechte
  - unzulässiger internationaler Datenverkehr
- bis zu 10 Mio € oder 2% des weltweiten Jahresumsatzes
  - Privacy by design/by default
  - Verletzung der Bedingungen der Auftragsverarbeitung
  - Datenschutz-Folgenabschätzung (→ Ausnahmen)
  - Verletzung der Bestellung eines DSB
- Im Datenschutz-Deregulierungsgesetz **„Abmahnung beim 1. mal“**
- **Reputation** “schlechte” Presse
- **Klagen**

Rollen & Datenströme



Begriffe

- Grundsätze
- Betroffene (Interessent, Kunden)
- Verantwortliche (Händler, Online-Händler, Agent, etc.)
- Auftragsverarbeiter (z.B. Druckerei)
- Datenkategorien (normale und sensible Daten)
- Empfänger von Daten
- Verfahrensverzeichnis
- Technisch Organisatorische Massnahmen (TOM)
  „Privacy by Design“ und „Privacy by Default“
- Datenschutzbeauftragter (brauche ich einen ?)
- Datenschutzverstöße – Meldung - Fristen

Rechte der Betroffener

Rechte

- Auskunft (binnen 1 Monat, 1x Jahr gratis)
- Berichtigung von Daten
- Einschränkung bei Speicherung/Verarbeitung
  wenn Rechtsgrund / Zweck weggefallen sind
- Löschung der Daten
  wenn Rechtsgrund / Zweck weggefallen sind
- Widerspruch zur Speicherung/Verarbeitung
  Ausnahme: wenn zwingende Interessen (z.B. Vertragserfüllung, Wahrung von Rechtsansprüchen) höher zu werten sind als Interessen des Betroffenen
- Widerruf der Einwilligung (für den jeweil. Zweck)
- Beschwerdemöglichkeit (bei der DSB)
- Datenübertragung an Dritte

Pflichten Verantwortlicher

Pflichten

- Rechtmäßigkeit (Rechtsgrund für die Verarbeitung, Zustimmung)
  - für Vertragserfüllung notwendig
  - für Erfüllung einer rechtlichen Verpflichtung notwendig
  - Lebenswichtiges Interesse des Betroffenen oder öffentliches Interesse
  - berechtigtes Interesse des Verantwortlichen oder eines Dritten, sofern nicht Interessen des Berechtigten überwiegen
  - Einwilligung (Koppelungsverbot; nicht vorangekreuzt)
- Transparenz, Treu und Glauben (Fairness)
  - Betroffener muss informiert sein(wer, was, warum, wohin, wie lange)
  - keine vorangekreuzten Checkboxen
  - keine Koppelungen
- Zweckbindung
- Speicherbegrenzung (Datenminimierung + Speicherdauer)
- Datenrichtigkeit
- Datensicherheit (**T**echnische und **O**rganisatorische Schutz**M**aßnahmen)
- Auskunftspflicht (Rechenschaftspflicht) gegenüber DSB und Betroffenen
- Dokumentations- & Schulungspflicht (->Verzeichnis)

Technisch-**O**rganisatorische **M**aßnahmen

Organisation & IT

- Vertraulichkeit
  - Zutrittskontrolle
  - Zugriffskontrolle
- Integrität
  - Eingabekontrolle
  - Weitergabekontrolle
  - Verschlüsselung
- Verfügbarkeit & Belastbarkeit
  - Sicherungskonzept, Backup-Strategie, Firewall, etc.
  - Datenschutzfreundliche Einstelllungen
- Regelmäße Überprüfung

Schritte bis 25. Mai 2018

→ Muster im Ordner DSGVO

1. **Analyse** Datenströme personenbezogene Daten

- Verarbeitungstätigkeiten / Datenanwendungen
- Rechtsgrundlagen
- Datenschutzbeauftragten / Datenschutzkoordinator

2. Maßnahmen nach AUSSEN

- Informationspflichten Website
- Cookie-Behandlung
- Datenschutzerklärung
- Anfrage/Bestellformulare
- Zustimmungserklärung
- AGB
- Newsletter-Anmeldung

3. Maßnahmen nach INNEN

- Verfahrensverzeichnis erstellen
- Datensicherheits-Maßnahmen
- ADV
- Auskunft/Rechte Betroffener
- Auskunft DSB
- DataBreach
- Schulung Mitarbeiter

Verfahrensverzeichnis

- **Namen und Kontaktdaten** des Unternehmens & Datenschutzbeauftragten,
- **Zwecke** der Datenverarbeitung,
- **Kategorien** betroffener **Personen,**
- **Kategorien** personenbezogener **Daten,**
- **Kategorien von Empfängern** von Daten,
- **Löschfristen** (nach Möglichkeit),
- Beschreibung **technischer & organisatorischer Datensicherheitsmaßnahmen,**
- ggf Übermittlungen von personenbezogenen Daten an ein **Drittland**
  - Angaben des Drittlands
  - Empfänger in Drittländern
  - geeignete Garantien

→ Muster im Ordner DSGVO

Verfahrensverzeichnis

Name und Kontaktdaten des/ der Verantwortlichen	Max Mustermann GmbH Neuer Weg 1 ZZZZ Musterdorf
Name und Kontaktdaten des Datenschutzbeauftragten	Franz Fachmann e.U. Datenstraße 5 YYYY Datenstadt

Merkmal eines Verfahrensverzeichnisses ist, dass die

datenverarbeitenden Unternehmensprozesse erfasst werden

und nicht die Anwendungen.

Zwecke der Daten-ver-arbeitung	Kategorien der Betroffenen	Kategorien personen-bezogener Daten	Kategorien von Empfängern	Empfänger in Drittländern	Fristen für die Löschung	technischen und organisatorischen Datensicherheits-maßnahmen
Personal-verwaltung	Mitarbeiter	Name, Adresse,...	GKK, Finanzamt,...		gesetz-liche Aufbe-wahrungs-fristen	Zutrittskontrolle, Zugriffskontrolle,...

Cookie

→ Muster Datenschutzerklärung im Ordner DSGVO

- § 96 Abs. 3 TKG
- Zustimmungserfordernis
  - um einen Dienst der vom Benutzer ausdrücklich gewünscht ist, zur Verfügung stellen zu können
- Informationspflicht (Betroffenenrechte DSGVO)
  - an „prominenter Stelle, in einfacher und klarer Sprache“ wie User Cookie akzeptieren kann
- welche personenbezogenen Daten ermittelt, verarbeitet und übermittelt werden
  - auf welcher Rechtsgrundlage
  - für welche Zwecke
  - Speicherdauer

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/checkliste-cookies-webanalyse-webshop.html

E-Mail Marketing

- Prüfen ob vorhandene Adressen „rechtmäßig“ erworben
- Prüfen ob Genehmigung (zweckgebunden) vorliegt
- Klare Regeln für Verwendungs-Zustimmung definieren
- Sorgfältige Auswahl Dienstleister und ADV abschließen
- Newsletter in AGB und Datenschutzerklärung aufnehmen
- Abwicklung der Auskunft ermöglichen (Formulare)

- Newsletter
  - Double-Opt-In
  - Nachweis des DOI / Einwilligung dokumentieren
  - nur E-Mail Adresse als Pflichtfeld (Grundsatz Datensparsamkeit)
  - Abmeldelink
  - Kopplungsverbot berücksichtigten
  - Impressum
  - das 1. E-Mail muss werbefrei sein

Einwilligung im Geschäft

→ Muster Datenschutzerklärung im Ordner DSGVO

Lieber Kunde,

sehr gerne möchten wir in gewohnter Weise weiterhin mit Ihnen in Kontakt bleiben und Sie mit Informationen aus unserem Autohaus _ _ CoKG auf dem Laufenden halten. Hierfür bedarf es aufgrund neuer datenschutzrechtlicher Regelungen, welche ab Mai 2018 in Kraft treten, Ihrer ausdrücklichen Einwilligung.

Datenschutzrechtliche Einwilligungserklärung

Ich bin damit einverstanden, dass meine oben angeführten personenbezogenen Daten sowie die damit in Verbindung stehenden Fahrzeugdaten für die nachfolgend ausgewählten Zwecke verwendet werden dürfen:

Zusendung von Informationen über Produkte, Dienstleistungen, Veranstaltungen sowie Marktforschungs- und Qualitätssicherungs-/verbesserungszwecken

☐ Post ☐ Telefon / SMS ☐ E-Mail ☐ kein Kontakt

Erinnerung an wichtige Werkstatttermine

☐ Post ☐ Telefon / SMS ☐ E-Mail ☐ kein Kontakt

.....

(Ort, Datum/Unterschrift)

Verträge mit Auftragsverarbeiter

- Gegenstand & Dauer der Verarbeitung
- Art & Zweck der Verarbeitung
- Art & Kategorien der Daten von Betroffenen
- Verpflichtung Vertraulichkeit
- Sicherstellung TOM
- Info über Subunternehmen
- Rückgabe & Löschung Daten nach Abschluss

→ Muster ADV im Ordner DSGVO

z.B. IT-Dienstleister, Cloudanbieter, Grafiker, Provider
→ Ausnahme Steuerberater, Handwerk

Der DSGVO Ordner

- 1_Informationen_DSGVO
  - DSGVO_Info-Folder-WKO.pdf
  - Speicher_und_Aufbewahrungsfristen.pdf
  - Webshop_Ablauf.pdf
  - Webshops-Verbraucherrechte.pdf
- 2_Verarbeitungsverzeichnis
  - Verarbeitungsverzeichnis_Online-Handel-Agent.docx
- 3_Auftragsverarbeiter-Vertrag
  - Auftragsverarbeiter-Vertrag.docx
- 4_Datenschutzerklaerung_Zustimmungserklaerung
  - Datenschutzerklaerung.docx
  - Zustimmungserklaerung_Datenverarbeitung.docx
- 5_Auskunft_Betroffene+DSB_DataBreach
  - Aushang_Beantwortung-von-Anfragen.docx
  - Beantwortung_Datenschutzanfrage.docx
  - DataBreach_Behoerde.docx
  - DataBreach_Betroffene.docx
  - Dienstanweisung_Datenschutzanfrage_Mitarbeiter.docx
  - Dienstanweisung_Vorgehen_Datenschutzverletzungen.docx
  - Erteilung_Auskunft.docx
  - Logbuch_Datenschutzanfragen.docx
- 6_Mitarbeiter
  - Datenschutzerklaerung_Mitarbeiter.docx
  - Datenschutzrichtlinie_Mitarbeiter.docx
  - Verpflichtung_Datengeheimnis.docx
  - WKO_Schulungsunterlagen_DSGVO.pdf

Links & Formulare

- https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig
- https://www.dsb.gv.at/dokumente
- https://ec.europa.eu/germany/news/20180126-neue-datenschutzregeln_de
- https://www.privacyshield.gov/list

§§

- https://dsgvo.wkoratgeber.at ← **Status-Check**
- http://meinnutzen.wko.at/infokit-datenschutz-grundverordnung/ ← **DSGVO Info-Kit**
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unterstuetzung-zur-Umsetzung-der-DSGVO.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Musterdokumente-zur-EU-Datenschutzgrundverordnung.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html
- https://www.wko.at/branchen/handel/datenschutzgrundverordnung-in-handelsunternehmen.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html
- https://www.bmf.gv.at/steuern/selbststaendige-unternehmer/betriebliches-rechnungswesen/br-aufbewahrungspflicht.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/checkliste-cookies-webanalyse-webshop.html