

DATENSCHUTZ-GRUNDVERORDNUNG FÜR IMMOBILIENMAKLER & IMMOBILIENVERWALTER



DSGVO - 25.05.2018

Unmittelbare Anwendbarkeit in allen EU-Mitgliedstaaten

Österreich: Adaptiertes Datenschutzgesetz zur Ergänzung der DSGVO

Schutz **personenbezogener** Daten

Anwendbar auf **jede** Verarbeitung personenbezogener Daten

Einzigste Ausnahme: Verarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten ("Haushaltsausnahme")

Unternehmensgröße oder Mitarbeiterzahl spielt keine Rolle

GRUNDBEGRIFFE

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Name, Adresse, e-mail Adresse, Telefonnummer, Foto, IP-Adresse)

Besondere Kategorien von Daten ("sensible Daten"):
z.B. Gesundheitsdaten, SV-Nummer, biometrische Daten, Religionsbekenntnis, Gewerkschaftszugehörigkeit, ethnische Herkunft, politische Meinung

Verarbeitung: jeglicher Umgang mit personenbezogenen Daten – digital und analog (u.a. Erheben, Erfassen, Organisation, Ordnen, Speicherung, Veränderung, Abfragen, Verwendung, Übermittlung, Verknüpfung, Löschen)

AKTEURE

Betroffene Person ("Betroffener"): Person, deren Daten verarbeitet werden

Verantwortlicher: Stelle, die allein oder gemeinsam mit anderen über die **Zwecke** und Mittel **der Verarbeitung** von personenbezogenen Daten entscheidet = Unternehmen, Vereine, Verbände, Behörden

Auftragsverarbeiter: Stelle, die personenbezogene Daten **im Auftrag** des Verantwortlichen verarbeitet, z.B.:

- Cloud-Computing
- Newsletterversand
- Datenerfassung, Datenkonvertierung
- Auslagerung der Lohn- und Gehaltsabrechnung
- Backup-Auslagerung und Archivierung

ÜBERMITTLUNG VON DATEN IN NICHT EU-LÄNDER

Der durch die DSGVO gewährte Schutz „reist“ mit den Daten, d.h. die Vorschriften gelten weiterhin, egal wohin die Daten übermittelt werden.

Übermittlung von Daten in Nicht-EU Länder ist daher nur unter folgenden Bedingungen zulässig

- Angemessenheitsbeschluss der Kommission, derzeit
 - **USA: Privacy-Shield Liste** <https://www.privacyshield.gov/list>
(zB Newsletterversand via US Anbieter – prüfen!)
 - Andorra, Argentinien, Färöer Inseln, Guernsey, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay
 - Partieller Angemessenheitsbeschluss: Kanada, Israel
- Geeignete Garantien (zB Standardvertragsklauseln, verbindliche interne Datenschutzvorschriften = Binding Corporate Rules)
- Ausnahmefälle (z.B. ausdrückliche Einwilligung)

GRUNDSÄTZE

DER VERARBEITUNG PERSONENBEZOGENER DATEN



ACCOUNTABILITY - RECHENSCHAFTSPFLICHT

Der Grundsatz der **Rechenschaftspflicht** ist ein Eckpfeiler der DSGVO:

Jedes Unternehmen ist für die Einhaltung aller Datenschutzgrundsätze **verantwortlich** und muss deren Einhaltung auch **nachweisen** können.

→ **Dokumentation** über:

- Einhaltung der Informationspflichten
- Umsetzung von Technischen und Organisatorischen Maßnahmen
- Abgegebene Einwilligungen
- Verarbeitungsverzeichnis
- Verträge mit Auftragsverarbeitern

VERARBEITUNGSVERZEICHNIS

Löst bisherige DVR-Meldungen als **rein interne Dokumentation** ab

Verarbeitungsverzeichnis ist schriftlich zu führen

→ kann ausdrücklich auch in einem elektronischen Format erfolgen
(z.B. Excel-Tabelle)

Dokumentation sämtlicher **Verarbeitungstätigkeiten**

→ keine Auflistung von Applikationen oder Programmen sondern
Zusammenfassung zusammengehöriger Vorgänge, in denen
personenbezogene Daten verarbeitet werden

Aktualisierungspflicht

INFORMATIONSPFLICHT

bei Erhebung von personenbezogenen Daten

= vor/bei **Vertragsabschluss**

- Umfassende Informationserteilung
- Einfache und klare Sprache
- Leicht zugänglich

→ **Datenschutzinformation** (im Vertrag selbst, Verweis auf Website, AGB)

Achtung: Information ist ausreichend für die Verarbeitung zur Erfüllung eines Vertrages - aber **nicht** wenn Daten auch zu anderen Zwecken, z.B. für Marketing, verwendet werden sollen

→ Zusätzlich **Einwilligung** einholen – auch hier:
Informationspflicht vor Einwilligung!

ZWECKBINDUNG

Im Zeitpunkt der Erhebung muss festgelegt sein, für welche Zwecke die personenbezogenen Daten verarbeitet werden

z.B. Kundenbetreuung, Newsletter, Abwicklung von Anfragen, Vertragsanbahnung und Vertragserfüllung

Durch die Angabe, wofür Daten verarbeitet werden, wird überprüfbar, ob die Verarbeitung konkreter Daten, für den jeweiligen Zweck notwendig ist

Verbot der Weiterverarbeitung von Daten zu anderen Zwecken

Ausnahme: Weiterverarbeitung für vorher vereinbare Zwecke

DATENMINIMIERUNG UND SPEICHERBEGRENZUNG

Datenminimierung: Verarbeitung nur jener Daten, die **für den jeweiligen Zweck notwendig** sind

Beispiel: um einen Newsletter zu versenden, benötigt man eine e-mail Adresse, nicht aber die Telefonnummer des Empfängers
→ Telefonnummer darf daher für diesen Zweck nicht erhoben werden

Speicherbegrenzung: Daten müssen so **kurz wie möglich** gespeichert werden. Der Zeitraum sollte die Gründe für die Verarbeitung der Daten sowie rechtliche Verpflichtungen zur Aufbewahrung der Daten für einen festgelegten Zeitraum berücksichtigen (z.B. 7 Jahre gem. BAO).

Daher: **Fristen zur Löschung oder Überprüfung** der gespeicherten Daten festlegen.

INTEGRITÄT UND VERTRAULICHKEIT

Bei der Verarbeitung muss die Sicherheit der Daten gewährleistet sein

→ **technische und organisatorische Maßnahmen (TOMs)** sind zu implementieren

Welche TOMs notwendig sind, kommt auf den konkreten Fall an

→ dabei zu berücksichtigen: Stand der Technik, Kosten der Implementierung, welche Daten werden wie oft und wofür verarbeitet usw.

Beispiele:

- Gebäudesicherung
- Alarmanlage
- Benutzername/Passwort
- Antiviren Software
- Verschlüsselung von (mobilen) Datenträgern

DATA PROTECTION BY DESIGN & BY DEFAULT

data protection by design

(= datenschutzfreundliche Technikgestaltung)

- Datenminimierung und Pseudonymisierung

data protection by default

(= datenschutzfreundliche Voreinstellungen)

→ Alles, wodurch mehr Daten verarbeitet werden, ist vom Nutzer zu aktivieren

- Optionale Felder als solche kennzeichnen
- "Ja, ich will den Newsletter erhalten" nicht vorangekreuzt

ERLAUBNIS ZUR VERARBEITUNG

Grundsatz:

Verarbeitung personenbezogener Daten ist verboten!

Nur erlaubt, wenn eine **Rechtsgrundlage** besteht:

- **Erfüllung eines Vertrages**
- **Rechtliche Verpflichtung**
- **Wahrung der berechtigten Interessen des Verantwortlichen**
- **Einwilligung**
- Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person
- Wahrnehmung einer Aufgabe, die öffentlichen Interesse liegt

VERTRAGSERFÜLLUNG

Verarbeitung der personenbezogenen Daten, die notwendig sind für

- den **Abschluss** oder
- die **Erfüllung** eines Vertrags

Andere Daten und/oder Zwecke → andere Rechtsgrundlage

Beispiel:

e-mail Adresse des Kunden wurde erhoben und gespeichert im Zusammenhang mit dem Abschluss eines Mietvertrages:

Verwendung für Übermittlung Rechnung Maklerprovision,
Dauerrechnung Miete, Betriebskostenabrechnung



Verwendung für Newsletter



ERFÜLLUNG EINER RECHTLICHEN VERPFLICHTUNG

Verarbeitung der personenbezogenen Daten, die notwendig sind für

- die **Erfüllung einer rechtlichen Verpflichtung**,
- welcher der **Verantwortliche unterliegt**

Beispiel:

Daten von Arbeitnehmern inklusive Sozialversicherungsnummer für
Anmeldung von Arbeitnehmern bei Sozialversicherungsträger

Selbstberechnung Grunderwerbsteuer: Sozialversicherungsnummer
für Finanz-Online

BERECHTIGTES INTERESSE

überwiegendes "*rechtliches, tatsächliches, wirtschaftliches oder ideelles Interesse*" des Verantwortlichen oder eines Dritten

Interessensabwägung zwischen Interessen des Verantwortlichen bzw. Dritten und jenen des Betroffenen:

Mit der Verfolgung der berechtigten Interessen dürfen die Rechte und Freiheiten Betroffener nicht ernsthaft beeinträchtigt werden, sonst kann der Verantwortliche sich nicht auf berechnigte Interessen berufen und muss eine andere Rechtsgrundlage finden.

→ Entscheidung im Einzelfall und daher Rechtsunsicherheit

EINWILLIGUNG

ANFORDERUNGEN

Mündlich & konkludent möglich aber: **Nachweispflicht !**

Einfache, klare Sprache und leicht zugänglich

Von anderen Sachverhalten klar unterscheidbar → **Hervorhebung**

Umfassende **Information** des Betroffenen (Informationspflicht)

Konkret einzelfallbezogene Einwilligungserklärung

"Ich stimme der Verarbeitung meiner e-mail Adresse zu Zwecken der Versendung eines Newsletters der XYZ GmbH zu "

Eindeutig bestätigende Handlung: Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit des Betroffenen stellt keine Einwilligung dar

→ **Aktives Verhalten des Betroffenen** erforderlich (Opt-In statt Opt-Out)

Hinweis auf **jederzeitiges Widerrufsrecht** ist verpflichtend

EINWILLIGUNGSERKLÄRUNGEN IN AGB

Koppelungsverbot

Sofern Daten verarbeitet werden sollen, die über den Zweck der Vertragserfüllung hinausgehen

→ **nicht in AGB**

→ **gesonderte Einwilligungserklärung**

Es muss die Möglichkeit gegeben werden, einen Vertrag auch ohne die Abgabe der datenschutzrechtlichen Zustimmungserklärung einzugehen
= Opt-in - Lösung

Beispiele:

In AGB enthaltene Einwilligung zur Verarbeitung der Daten zu Werbezwecken ist unzulässig

In einem Angebotsformular ist die Einwilligung des Kunden zur Verwendung seiner Daten zu Marketingzwecken enthalten. Einwilligung ist unwirksam.

EINWILLIGUNG



- vorab angekreuzte Kästchen
- Untätigkeit des Betroffenen
- unbestimmter Zweck der Verarbeitung – nicht: z.B. ...
- Einwilligung in AGB
- Koppelung mit Vertragsabschluss
- Belohnungen
- Verzicht auf Betroffenenrechte



- Ankreuzen eines Kästchens
- Einwilligung durch Erklärung
- Konkreter Zweck der Verarbeitung beschreiben
- Einwilligung gesondert unterschreiben/anklicken
- Einwilligung ist unabhängig vom Vertragsabschluss
- Information über Widerruf
- Information über sonstige Rechte

ÜBERMITTLUNG VON DATEN AN DRITTE

Verarbeitet der Empfänger die Daten **auch für eigene Zwecke**, muss die Übermittlung ebenso auf einer Rechtsgrundlage basieren. Somit ist die Datenübermittlung rechtmäßig und zulässig:

- zur Vertragsanbahnung oder Vertragserfüllung erforderlich
- es liegt eine gesetzliche Verpflichtung vor
- es gibt eine Einwilligung des Betroffenen

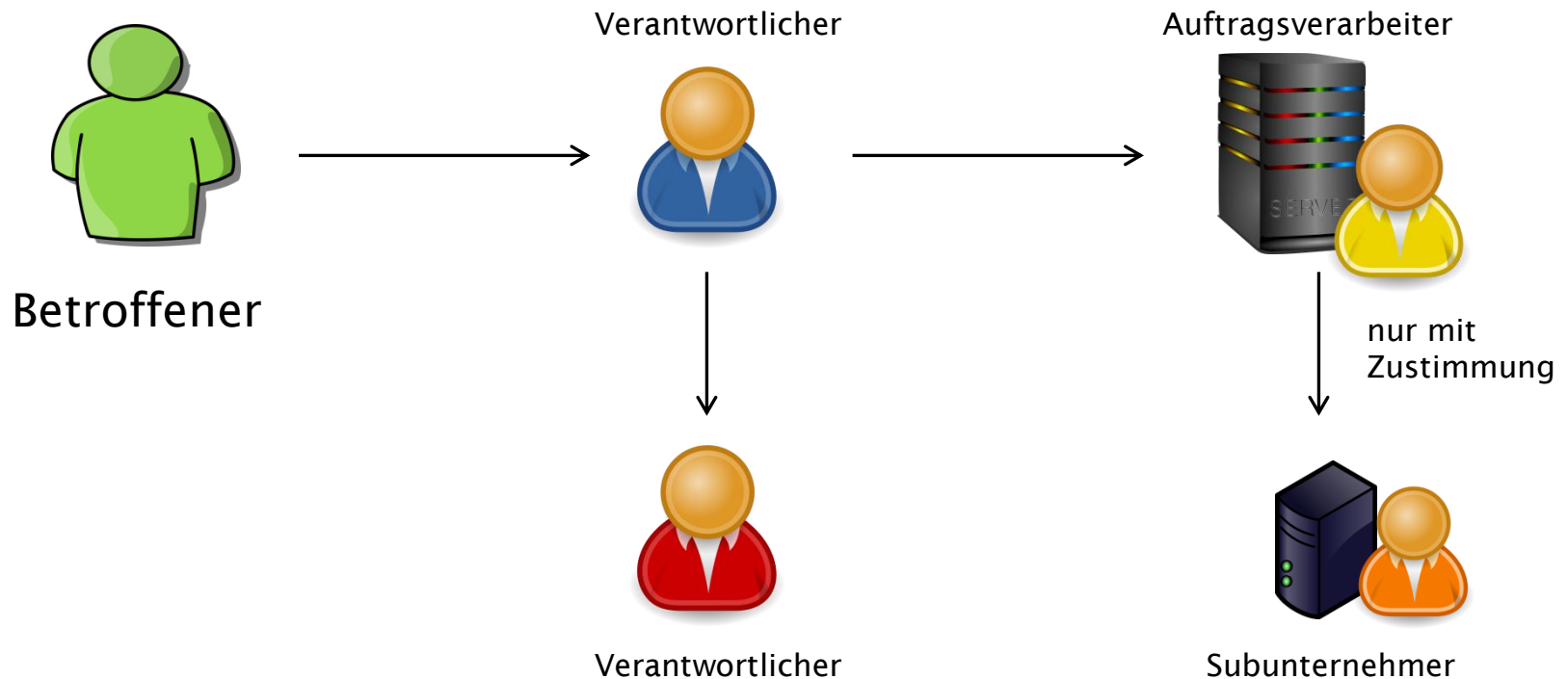
Verarbeitet der Empfänger die Daten **im Auftrag eines anderen** (zB externe Druckdienstleistung, Rechenzentrum, IT Provider) ist keine Rechtsgrundlage erforderlich.

Aber es muss ein schriftlicher Vertrag mit dem Auftragsverarbeiter mit bestimmten Mindestanforderungen abgeschlossen werden.

Und wie immer: **Informationspflicht!**

EXTERNE DIENSTLEISTUNGEN

Auftragsverarbeiter oder Verantwortlicher?



AUFTRAGSVERARBEITER

Verarbeitung **im Auftrag** des Verantwortlichen

- "verlängerter Arm" des Verantwortlichen
- Entscheidung über die Verarbeitungszwecke trifft Verantwortlicher
- Auftragsverarbeiter ist weisungsgebunden
- Auftragsverarbeiter hat (technische) Hilfs-/Unterstützungsfunktion
- Verarbeitung durch den Auftragsverarbeiter wird grundsätzlich dem Verantwortlichen zugerechnet
- Daher: keine Rechtsgrundlage für Weitergabe der Daten nötig

Beispiele: Cloud-Computing, externe Druckdienstleistung, Backup-Sicherheitsspeicherung und Archivierungen, Lohnverrechnung, Fernwartung, externer Support für IT-System

Nicht jeder externe Dienstleister ist ein Auftragsverarbeiter!

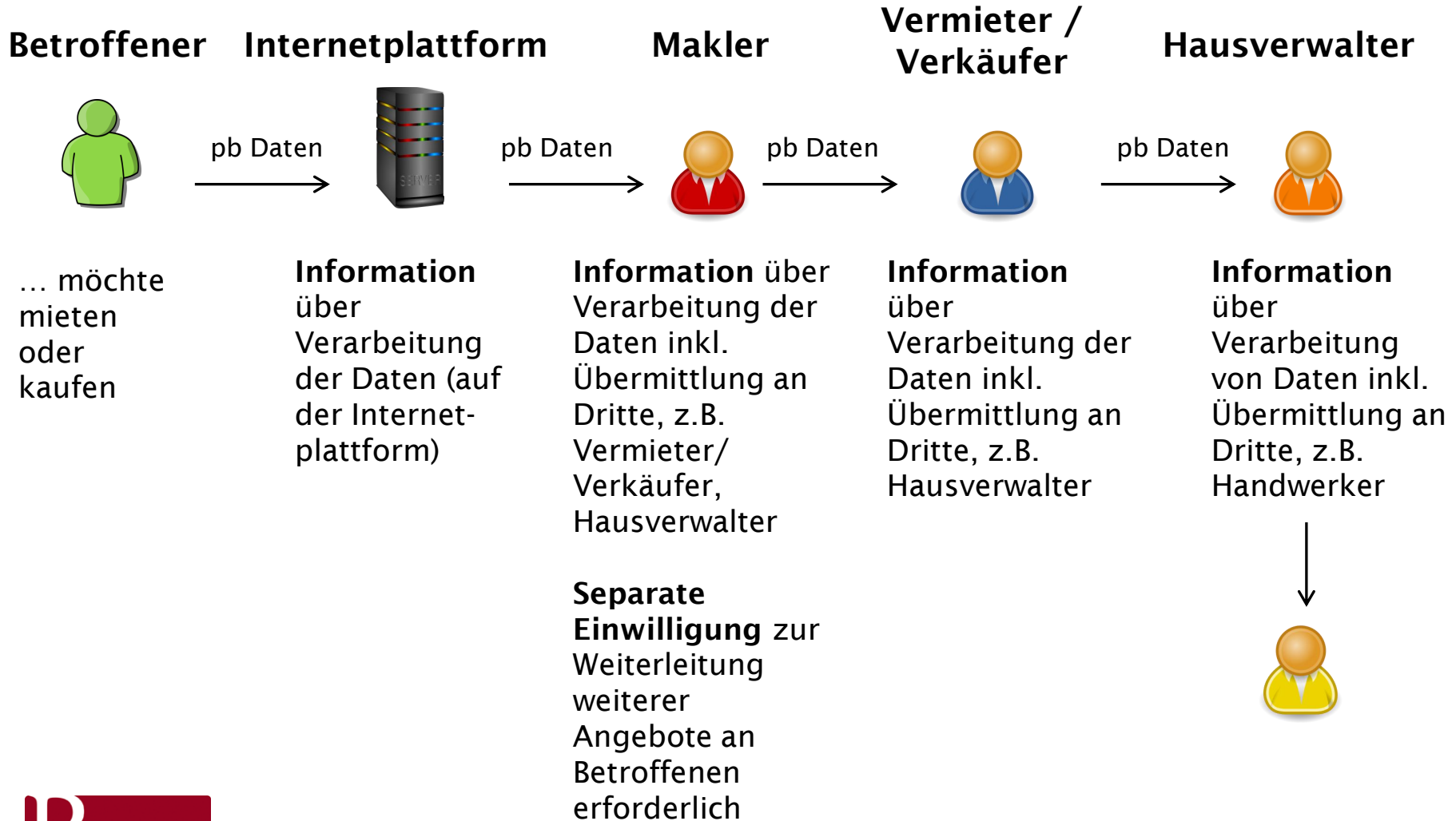
BEAUFTRAGUNG EINES AUFTRAGSVERARBEITERS

Beauftragung nur solcher Auftragsverarbeiter, die Einsatz **DSGVO-konformer TOMs garantieren**

- Einhaltung genehmigter Verhaltensweisen oder anerkannter Zertifizierungen als Faktor
- Abschluss eines **Vertrages ist verpflichtend**
- Zwingend schriftlich (auch in elektronischer Form)
- Bestehende Verträge mit Laufzeit nach dem 25.05.2018 sind mit Nachtrag anzupassen
- **Mindestinhalt** in Art 28 DSGVO

Auftragsverarbeiter muss ebenfalls ein Verarbeitungsverzeichnis führen

DATENFLUSS



SONSTIGE PFLICHTEN

Datenschutzbeauftragter

- Bei umfangreicher regelmäßiger und systematische Überwachung von Betroffenen oder bei umfangreichen Verarbeitungen sensibler Daten oder Daten über strafrechtliche Verurteilungen (z.B. Banken, Versicherungen)
- Sonst: freiwillige Benennung

Datenschutz-Folgenabschätzung

- Wenn aufgrund der Art, des Umfangs und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Betroffenen besteht

Data Breach Notification

- Meldung von Datenpannen an Aufsichtsbehörde und ggf. Betroffene

WEBSITE, NEWSLETTER UND SOCIAL MEDIA



WEBSITE

Zusätzlich zu DSGVO anwendbar:

Unternehmensgesetzbuch (UGB), E-Commerce Gesetz (ECG),
Mediengesetz, Telekommunikationsgesetz (TKG)

→ Impressumspflicht

IP-Adressen gelten als personenbezogene Daten

Datenschutzrechtlich relevante Inhalte sind z.B.

- Cookies und Web-Analyse-Tools
- Registrierung
- Newsletter
- Kontaktformular
- Bestellungen
- Gewinnspiele

DATENSCHUTZERKLÄRUNG

Informationspflicht zum Zeitpunkt der Erhebung von personenbezogenen Daten

- Einfache und klare Sprache
- Leicht zugänglich

→ **Datenschutzerklärung** auf der Website

Information über **sämtliche datenschutzrechtlich relevanten Inhalte** auf der Website

Achtung: lediglich Erfüllung der Informationspflicht
u.U. ist auch eine Einwilligung einzuholen

KONTAKTFORMULAR

ALLGEMEINES

Informationspflicht bei Erhebung der personenbezogenen Daten

→ Link zur **Datenschutzerklärung**, die sich idealerweise im Abschnitt "Kontaktformular" öffnet

Grundsätzlich keine Einwilligung erforderlich

→ "**Berechtigtes Interesse**" des Websitebetreibers

Datenminimierung: **nur erforderliche Daten als Pflichtfelder**

Verarbeitung **nur zu Zwecken** der Bearbeitung der **Kontaktanfrage**

KONTAKTFORMULAR

BEISPIEL

Anrede* ▼

Vorname*

Nachname*

Kundennummer

Wählen Sie Ihr Land*
Österreich ▼

E-Mail Adresse*

Telefonnummer

Postleitzahl

☐ Alle Informationen werden vertraulich behandelt. Für weitere Informationen lesen Sie bitte die [Datenschutzpolitik](#).

SENDEN



WERBUNG, NEWSLETTER

Reminder: § 107 TKG - unzulässig ist:

- Cold Calling
- „Spamming“ - Zusendung elektronischer Post (auch SMS) ohne vorherige Einwilligung, wenn Zusendung zu Zwecken der Direktwerbung erfolgt oder an mehr als 50 Empfänger gerichtet ist

Telefonnummern und e-mail Adressen sind personenbezogene Daten
→ DSGVO ist anwendbar

Für Zusendung Newsletter/Werbung: **Einwilligungserklärung** erforderlich

Nachweisbarkeit der Einwilligung z.B. durch "Double-Opt-In"

SOCIAL MEDIA

Social Media Plug-Ins

- Einwilligung erforderlich
- Besucher kann nicht darüber informiert werden, welche Daten vom sozialen Netzwerk genau erhoben werden und was mit ihnen geschieht

→ **Gültige Einwilligung nicht möglich**

Alternative 1: **Verzicht auf Social Media Plug-Ins**

Alternative 2: **"2-Klick"-Lösung**

Problem: Information nicht möglich

Alternative 3: **"Shariff"-Lösung**

Vorteil: Informationspflicht trifft soziales Netzwerk

SOCIAL MEDIA

BEISPIEL

Gefällt Dir
der Artikel?
Bitte teile ihn!

 tweet	204
 teilen	38
 +1	4k

 tweet	15k
 tweet	99
 tweet	15k

 teilen	689
 share	82
 teilen	689

 +1	272k
 +1	12k
 +1	272k

RECHTE DER BETROFFENEN



RECHTE DER BETROFFENEN

Anträge von Betroffenen bedürfen **keiner besonderen Form**

Beantwortung **innen eines Monats**

Verlängerung um zwei weitere Monate mit Begründung möglich

Grundsätzlich **kostenlos**

Außer bei offenkundig unbegründeten oder exzessiven Anträgen
(Verweigerung möglich)

Identitätsnachweis durch Betroffenen erforderlich

Bei begründeten Zweifeln (aber nur dann!) Anforderung zusätzlicher
Informationen zur Identität z.B. telefonische Anfrage oder Anfrage über
eine bisher unbekannte e-mail Adresse

Grundsätzlich **schriftliche v.a. elektronische** Auskunftserteilung

→ **Einführung eines Systems zur fristgerechten Bearbeitung von
Anträgen**

RECHT AUF AUSKUNFT

Auskunft über:

- Verarbeitungszweck(e) (empfehlenswert: auch Rechtsgrundlage)
 - Kategorien personenbezogener Daten
 - Empfänger / Kategorie von Empfängern
 - Speicherdauer bzw. wenn nicht möglich Kriterien zu deren Festlegung
 - Die (weiteren) Betroffenenrechte
 - Das Bestehen eines Beschwerderechts bei der DSB
 - Vorliegen automatisierter Entscheidungsfindung und Profiling
- Im Wesentlichen Inhalt der allgemeinen Informationspflicht

Bei Verlangen auch Bereitstellung einer Datenkopie

RECHT AUF LÖSCHUNG

Recht auf Löschung, insb. wenn

- Personenbezogene Daten für die Zwecke nicht mehr notwendig sind
- Der Betroffene seine Einwilligung widerruft und keine andere Rechtsgrundlage vorliegt
- Personenbezogene Daten unrechtmäßig verarbeitet wurden
- Die Löschung gesetzlich vorgesehen ist

Gründe für Ablehnung, insb.:

- Erfüllung einer rechtlichen Verpflichtung
- Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

WEITERE BETROFFENENRECHTE

- Recht auf Widerspruch
- Recht auf Berichtigung
- Recht auf Einschränkung / Sperrung
- Recht auf Datenübertragbarkeit

HAFTUNG, STRAFEN



AUFSICHTSBEHÖRDE

In Österreich ist die **Datenschutzbehörde (DSB)** die nationale Aufsichtsbehörde

Untersuchungsbefugnisse, z.B. Aufklärungen verlangen, Einschau in Datenverarbeitungen und Unterlagen, Räume betreten, Kopien von Datenträgern herstellen

Abhilfebefugnisse, z.B. konkrete Anordnungen, Verhängung von Geldbußen (Verwaltungsstrafen)

Beschwerderecht von Betroffenen bei der DSB

Betroffene können sich von (Datenschutz)NGOs vertreten lassen

DSB entscheidet verbindlich, Rechtszug an Bundesverwaltungsgericht

VERGLEICH HÖHE DER GELDBUßEN

DSG 2000 - DSGVO

Verstoß / Übertretung	Höchstbuße	bisher (max. Geldstrafe)
unrechtmäßige Datenspeicherung	EUR 20.000.000,- oder 4 % v. Umsatz	nicht strafbar
Verletzung des Auskunftsrechts / Löschungsrechts	EUR 20.000.000,- oder 4 % v. Umsatz	EUR 500,-
unzulässige Auslandsübermittlung	EUR 20.000.000,- oder 4 % v. Umsatz	EUR 10.000,-
mangelhafte Datensicherheit	EUR 10.000.000.- oder 2 % v. Umsatz	EUR 10.000,-
fehlender Auftragsverarbeitervertrag	EUR 10.000.000,- oder 2 % v. Umsatz	nicht strafbar

STRAFRAHMEN GELDBUßEN

bis zu 20 Mio. EUR oder 4 % des weltweit erzielten Jahresumsatzes

Geldbußen sollen nach der DSGVO in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sein

Zur **konkreten** Festlegung einer angemessenen Geldbuße wird jeder Fall anhand einer Reihe von Faktoren geprüft, dazu gehören:

- die Schwere/Dauer des Verstoßes
- die Zahl der betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens
- die Vorsätzlichkeit des Verstoßes
- Maßnahmen zur Minderung des entstandenen Schadens
- der Umfang der Zusammenarbeit mit der Aufsichtsbehörde

KLAGEN

Klagen auf Unterlassung

Schadenersatz wegen materieller und immaterieller Schäden

- Beweislast trifft Verantwortlichen / Auftragsverarbeiter
- Solidarhaftung aller beteiligten Verantwortlichen / Auftragsverarbeiter
- Mögliche Kläger: Betroffene, können sich durch Datenschutz-NGOs oder Schutzverbände vertreten lassen

Klagen nach UWG

- Mögliche Kläger: Konkurrenten und Schutzverbände

DSGVO - TO DOs

- Erfüllung und Dokumentation der Informationspflichten
- Erstellen eines Verarbeitungsverzeichnisses
- Anpassung der Homepage
- Anpassung AGB
- Newsletter/Direktmarketing: Einwilligungen?
- Anbieterauswahl externe Dienstleister (außerhalb EU?)
- Verträge mit Auftragsverarbeitern
- Implementierung und Dokumentation der TOMs
- Konzept für Umgang mit Betroffenenrechten
- Aufbewahrungsfristen und Löschkonzept
- Notfallkonzept bei Datenpannen

LINKS

DSGVO

<http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679>

Datenschutzangemessenheits-Verordnung

<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000312>

Privacy-Shield Liste

<https://www.privacyshield.gov/list>

Datenschutzbehörde

<https://www.dsb.gv.at>



MMag. Birgit Harasser



Kimon Koussoulis, LL.M.

Brand Rechtsanwälte GmbH

Schüttelstr. 55, 1020 Wien

office@b-law.at +43 1 725 77 www.datenschutz2018.at