Datenschutz

20. Feber 2020

Dr. Kurt Einzinger

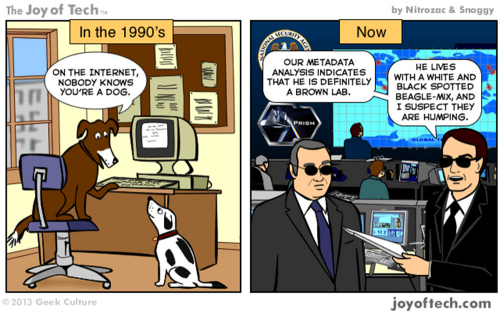
Dr. Kurt Einzinger

- Technologisches Gewerbe Museum (TGM) Wien, Fachbereich Atomenergietechnik
- Doktorat Ethnologie Universität Wien (Diss: Sikhs in Indien)
- EDV-Leiter einer politischen Partei (1989 – 1996)
- EDV-Abteilungen von Banken (GiroCredit, EB, OeKB)
- Generalsekretär der ISPA (Internet Service Providers Austria) – EuroISPA (Brüssel)
- Mitglied des Österreichischen Datenschutzrates (seit 1990)
- Member of Advisory Group of ENISA (European Network and Information Security Agency) (2004-2008, 2017-2020)
- Cyber Security Forschungsprojekte (CAIS, CIIS,CISA)
- netelligenz – Datenschutz und Cyber Security Beratung
- Externer Datenschutzbeauftragter

Disclaimer

On the Internet,
Nobody Knows You're a Dog

page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20)



Haftungsausschluß: Die Thesen und Ausführungen des Vortrags stellen ausschließlich die Meinung und Ansichten des Vortragenden dar. Für deren Inhalt wird keinerlei Haftung übernommen. Die darin enthaltenen Informationen stellen keine Rechts-, Anlage- oder sonstige Beratung dar, noch sollten auf Grund dieser Angaben Anlage- oder sonstige Entscheidungen gefällt werden, sondern sie gelten lediglich als unverbindliche Information.

Inhalt

- Worum geht‘s ?
  Grundbegriffe des Datenschutzes
- Rechtskonstruktionen und Institutionen
- DSGVO Grundsätze und Anforderungen
- Ausgewählte Kapitel
  - Fotos - Videoüberwachung
  - Pseudonymisierung und Anonymisierung
  - Direktwerbung - Spam
  - Cookies
  - Facebook Pixel

Grundbegriffe des Datenschutzes

personenbezogene Daten

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, (Art 4 lit 1 DSGVO)

Verarbeitung

bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; (Art 4 lit 2 DSGVO)

Verantwortlicher und Auftragsverarbeiter

Im DSG 2000: „Auftraggeber“ und „Dienstleister“

Artikel 4 DSGVO: Begriffsbestimmungen

7. „Verantwortlicher“ die 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
8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
9. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

Datenschutzgesetz – DSG

Anwendungsbereich und Durchführungsbestimmung

§ 4 (1) Die Bestimmungen der DSGVO und dieses Bundesgesetzes gelten für die **ganz oder teilweise automatisierte** Verarbeitung personenbezogener Daten natürlicher Personen sowie für die **nichtautomatisierte** Verarbeitung personenbezogener Daten natürlicher Personen, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen,…

DSGVO Nicht-Anwendungsbereich

Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

- durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, (Art 2 DSGVO)
- juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person. (Erwägungsgrund 14 DSGVO)
- Verstorbener (keine natürliche Person)

besondere Kategorie personenbezogener (sensible) Daten

Die Verarbeitung personenbezogener Daten, aus denen die *rassische und ethnische Herkunft*, *politische Meinungen, religiöse oder weltanschauliche Überzeugungen* oder die *Gewerkschaftszugehörigkeit* hervorgehen, sowie die Verarbeitung von *genetischen Daten, biometrischen Daten* zur eindeutigen Identifizierung einer natürlichen Person, *Gesundheitsdaten* oder *Daten zum Sexualleben oder der sexuellen Orientierung* einer natürlichen Person ist untersagt. (Art 9 DSGVO)

Rechtskonstruktionen und Institutionen

EMRK

Europäische Konvention zum Schutz der Menschenrechte und Grundrechte (Verfassungsrang - in Österreich in Kraft seit 3.9.1958)

Artikel 8: Recht auf Achtung des Privat- und Familienlebens

Abs.1: Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

Abs.2: Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Charta der Grundrechte der EU (seit 2000)

Artikel 8 Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Neuer Rechtsrahmen der EU

- Datenschutz-Grundverordnung DSGVO 2016/679 (seit 25.5.2016 in Kraft)
  - gilt nur wo die EU Kompetenz hat
  - seit 25.5.2018 gilt sie in allen EU-Staaten
- Richtlinie für Strafverfolgung und justiziellen Bereich (DS-RL 2016/680)
  - umgesetzt im 3.Hauptstück des DSG
- e-Privacy Richtlinie (RL 2002/58/EG und RL 2009/136/EG) soll e-Privacy Verordnung werden
  - Lex Specialis zur DSGVO
  - Frühestens Anfang 2021 (+ Übergangsfrist)

Datenschutz als Grundrecht

Erwägungsgrund 1 DSGVO:
Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Rechtslage Österreich

- Datenschutzgesetz DSG 2000 (seit 1.1.2000)
- Datenschutzgesetz (DSG) ab: 25.5.2018
  DSG, BGBLA 2017/1/120, 31.7.2017
  - Gesamtändernder Abänderungsantrag (im Ausschuss 26.6.17)
    Novellierung des DSG 2000
    Verfassungsbestimmungen bleiben
- Datenschutz-Deregulierungsgesetz
  - 3-Parteienantrag zur Änderung des DSG (Verfassungsbest.)
  - Abänderungsantrag im Plenum am 20.4.18 (Verfassungsbest. bleiben, Änderungen Medienunternehmen und Verwarnung)
- Datenschutzanpassungsgesetze zur Anpassung der Materiengesetze

Rechtsvorrang der EU

- nationale Bestimmungen sind richtlinienkonform auszulegen (nach der ständigen Rechtsprechung des EuGH)
- Die unmittelbare Anwendbarkeit (Wirksamkeit) von unionsrechtlichen Bestimmungen ist von jeder Verwaltungsbehörde bzw. von jedem nationalen Gericht zu beachten.
- Dabei ist zu beachten ob die nationale Regelung, die Intention der Richtlinie auf anderem Wege erreicht, oder nicht

Datenschutzbehörde DSB

www.dsb.gv.at

- Nationale Aufsichtsbehörde (Art 51 DSGVO)
- Unabhängig und Weisungsfrei (im BMVRDJ)
- kann Einschau in Datenverarbeitungen und diesbezügliche Unterlagen begehren.
- ist berechtigt Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen und die zu überprüfenden Verarbeitungen durchzuführen.
- kann die Weiterführung der Datenverarbeitung untersagen (Gefahr im Verzug).
- kann Geldbußen verhängen.

Datenschutzrat

- nimmt zu Fragen von grundsätzlicher Bedeutung für den Datenschutz Stellung, fördert die einheitliche Fortentwicklung des Datenschutzes und berät die Bundesregierung in rechtspolitischer Hinsicht bei datenschutz-rechtlich relevanten Vorhaben.
- Mitglieder: pol. Parteien (12), AK & WKO (je 1), Länder (2), Gemeindebund & Städtebund (je 1), BMVRDJ (1), DPO-Bund (1), Experten (2) - für eine Legislaturperiode
- kann Auskunftspersonen laden
- Nimmt Stellung bei Gesetzesbegutachtungen

DSGVO – Rechtsdurchsetzung

- Datenschutzbeauftragter (Art 37-39)
- Verwaltungsgerichte (Land, Bund)
- Unabhängige Aufsichtsbehörde DSB (Art 51ff)
- Europäischer Datenschutzausschuss (Art 68ff)
- Betroffenenrechte (Art 15-23)
- Recht auf Beschwerde bei Behörde (Art 77)
- Haftung und Recht auf Schadenersatz (Art 82)
- Verwaltungsrechtliche Sanktionen der Behörde (Art 83) – wirksam, verhältnismäßig und abschreckend (bis zu 20 Mio € od. 4% vom Jahresumsatz weltweit)

Verwarnung durch die Datenschutzbehörde (DSG)

§ 11 Die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO (Befugnisse der Aufsichtsbehörde) von ihren Abhilfebefugnissen insbesondere durch **Verwarnen** Gebrauch machen.

Offene Frage: ob EU-Rechts konform?

DSGVO Grundsätze und Anforderungen

Bei Verarbeitung zu tun

- Zwecke der Verarbeitung festlegen
- Rechtsgrundlagen definieren (Rechtmäßigkeit)
- Datenkategorien bestimmen (Sensible Daten?)
- Mit Auftragsverarbeiter Vereinbarung abschließen
- Falls notwendig, Datenschutzfolgeabschätzung
- Löschkonzept erstellen
- Betroffeneninformation bei Daten-Erhebung und in Datenschutzerklärung
- Ins Verzeichnis von Verarbeitungstätigkeiten eintragen
- Sicherheit der Verarbeitung sicherstellen

Grundsätze für die Verarbeitung personenbezogener Daten (Art 5 DSGVO)

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
2. Zweckbindung;
3. Datenminimierung;
4. Richtigkeit;
5. Speicherbegrenzung – nur so lange als nötig;
6. Integrität und Vertraulichkeit - Sicherheit;
7. Rechenschaftspflicht

Rechtmäßigkeit der Verarbeitung (Art 6 DSGVO)

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; (Nachweispflicht)

b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung **vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen;

Rechtmäßigkeit der Verarbeitung (2)

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung **öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Sensible Daten (2)

Verbot der Verarbeitung besonderer Kategorien personenbezogener (sensibler) Daten

– gilt nicht in folgenden Fällen:

die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

Löschung

Personenbezogene Daten müssen unwiderruflich gelöscht oder anonymisiert werden wenn

a) sie für den Zweck der Verarbeitung nicht mehr benötigt werden (keine Rechtsgrundlage mehr),
b) keine gesetzliche Verpflichtung zur Aufbewahrung besteht,
c) die Einwilligung widerrufen wird (bei auf Einwilligung beruhenden Verarbeitungen)
d) das Recht auf Löschung geltend gemacht wird und Punkt a und b zutrifft

Löschung (2)

§ 4 (2) DSG

Kann die **Berichtigung oder Löschung** von automationsunterstützt verarbeiteten personenbezogenen Daten **nicht unverzüglich erfolgen**, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt **einzuschränken.**

Verzeichnis von Verarbeitungstätigkeiten (1)

Artikel 30 (1) Jeder Verantwortliche (auch Auftragsverarbeiter in geringerem Umfang) führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

Verzeichnis von Verarbeitungstätigkeiten (2)

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen.

Es bestehen keine Formvorschriften (schriftlich oder elektronisch)

Es muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden. (Anstelle der DVR Eintragung)

Bei > 250 Mitarbeiter, es sei denn die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien

Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungs-vorgänge für den Schutz personenbezogener Daten durch.

Der Rat des Datenschutzbeauftragten ist einzuholen

Datenschutz-Folgenabschätzung (2)

ist in folgenden Fällen erforderlich:

- Bei systematischer und umfassender Bewertung persön-licher Aspekte natürlicher Personen, die sich auf auto-matisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
- Bei umfangreiche Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten
- Bei systematischer, umfangreicher Überwachung öffentlich zugänglicher Bereiche.

Negativ und positiv Verordnungen der DSB:
https://www.dsb.gv.at/verordnungen-in-osterreich

Rechte der betroffenen Person

- Auskunftsrecht der betroffenen Person (Art 15)
- Recht auf Berichtigung (Art 16)
- Recht auf Löschung (Art 17)
- Recht auf Einschränkung der Verarbeitung (Art 18)
- Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art 19)
- Recht auf Datenübertragbarkeit (Art 20)
- Widerspruchsrecht (Art 21)
- Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art 22)

Information bei Anfragen

- Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Betroffenenrechten unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung.
- Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.
- Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung.
- Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

Information bei Anfragen (2)

Informationen werden unentgeltlich zur Verfügung gestellt.

Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen kann der Verantwortliche entweder

- ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
- sich weigern, aufgrund des Antrags tätig zu werden.
- Der Verantwortliche hat Nachweis für den unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

Bei begründeten Zweifel an der Identität des Betroffenen, können zusätzliche Informationen angefordert werden.

Auskunftsausnahmen (DSG)

§4 (5) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem **hoheitlich tätigen Verantwortlichen** unbeschadet anderer gesetzlicher Beschränkungen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

§ 4 (6) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen in der Regel dann nicht, wenn durch die Erteilung dieser Auskunft ein **Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter** gefährdet würde.

Informationspflichten (Art 12 DSGVO)

- Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen bei Erhebung oder Erlangung der personenbezogenen Daten und alle Mitteilungen gemäß den Betroffenenrechten, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.
- Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.
- Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.
- Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte

Informationspflicht (Art 13 DSGVO)

Artikel 13 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so **teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes** mit:

a) Namen und Kontaktdaten des Verantwortlichen
b) Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
c) Zwecke und Rechtsgrundlagen der Verarbeitung
d) Wenn die Verarbeitung auf **Art 6 Abs 1 lit f DSGVO** beruht, die berechtigten Interessen die von dem Verantwortlichen oder einem Dritten verfolgt werden
e) Empfänger oder Kategorien von Empfängern (wenn vorhanden)
f) Absicht, personenbezogene Daten an ein Drittland oder internationale Organisation zu übermitteln (wenn vorhanden)

Informationspflicht (Art 13 DSGVO) 2

(2) Zusätzlich zu den Informationen gemäß Absatz 1
a) Speicherdauer
b) Auskunftsrecht, Recht auf Berichtigung und Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit
c) Recht die Einwilligung zu widerrufen
d) Beschwerderecht bei der Aufsichtsbehörde (Datenschutzbehörde DSB)
e) Rechtsgrundlage der Verpflichtung der Bereitstellung der personenbezogenen Daten bei Vertragsabschluss und mögliche Folgen bei Nichtbereitstellung
f) Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (wenn vorhanden)

Informationspflicht (Art 14 DSGVO)

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person folgendes mit:

- Namen und Kontaktdaten des Verantwortlichen (bzw. Vertreters)
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- die Verarbeitungszwecke, sowie deren Rechtsgrundlage
- die Kategorien personenbezogener Daten, die verarbeitet werden
- gegebenenfalls die Empfänger oder Kategorien von Empfängern
- gegebenenfalls die Absicht, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

Informationspflicht (Art 14 DSGVO) 2

- längstens innerhalb eines Monats,
- falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
- falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.
- Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung.

Keine Informationspflicht, wenn

- die Betroffenen bereits über die Informationen verfügen
- die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, oder
- die genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. Der Verantwortliche muss dann geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der Betroffenen ergreifen.
- die Erlangung der Daten durch Rechtsvorschriften, denen der Verantwortliche unterliegt ausdrücklich geregelt ist
- oder die Daten dem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegen und vertraulich behandelt werden müssen.

Information auf Website

Datenschutzerklärung (Privacy Policy) – empfohlen
- Von allen Seiten erreichbar (wie Impressum)
- Allgemeine Erklärung, wie von dem Unternehmen personenbezogene Daten verarbeitet werden
- Hinweis auf Betroffenenrechte, Beschwerdemöglichkeit
- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten (falls vorhanden)
- Beschreibung wie die Website mit personenbezogenen Daten verfährt
  - Log-Files
  - Cookies
  - Social Embeddings etc.

Informationstext bei Formularen, wo personenbezogene Daten erhoben werden – Link zur Datenschutzerklärung

Auftragsverarbeiter (Art 28 DSGVO)

Der Auftragsverarbeiter muss Garantien dafür bieten,
- dass geeignete technische und organisatorische Maßnahmen durchgeführt werden,
- dass die Verarbeitung im Einklang mit der DSGVO erfolgt
- dass der Schutz der Rechte der betroffenen Personen gewährleistet ist

Auftragsverarbeitungsvereinbarung (Vertrag) legt fest:
- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen und
- die Pflichten und Rechte des Verantwortlichen
- Sub-Auftragsverarbeiter nur mit Zustimmung des Verantwortlichen

Mitarbeiterverpflichtung

Ich verpflichte mich, die Vorschriften des Datenschutzgesetzes sowie der DSGVO zu wahren und den Datenschutz und die Datensicherheit unabhängig davon, ob es sich um gesetzliche Verpflichtungen oder um betriebliche Anordnungen handelt, einzuhalten.

a) Datengeheimnis gemäß § 6 DSG zu wahren - auch nach Beendigung meines Arbeitsverhältnisses
b) dass die verarbeiteten Daten eine besondere Kategorie personenbezogener Daten darstellen (falls zutreffend)
c) nur aufgrund einer ausdrücklichen Anordnung meines Arbeitgebers (Dienstgebers) personenbezogene Daten verarbeiten darf
d) dass ich das Recht habe eine unzulässige Datenübermittlung zu verweigern und mir daraus kein Nachteil erwachsen darf
e) jede Verletzung des Schutzes personenbezogener Daten, die mir bekannt geworden ist, unverzüglich meinem Arbeitgeber zu melden.

Im besonderen verpflichte ich mich zur sorgfältigen Verwahrung von Benutzerkennwörtern, Passwörter und sonstiger Zugangsberechtigungen.

Meldepflicht (Art 33 DSGVO)

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten **meldet der Verantwortliche unverzüglich** und **möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde**, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt**. Erfolgt die Meldung an die Aufsichtsbehörde **nicht binnen 72 Stunden**, so ist ihr eine **Begründung für die Verzögerung beizufügen**.

(2) Wenn dem Auftragsverarbeiter eine Verletzung bekannt wird – **meldet** er diese dem Verantwortlichen **unverzüglich**

Meldepflicht (Art 34 DSGVO)

(1) Hat die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge – muss der Verantwortliche die betroffenen Personen unverzüglich benachrichtigen.

(3) Die Benachrichtigung ist nicht erforderlich wenn einer der folgenden Bedingung erfüllt ist

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat

b) der Verantwortliche durch Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person, aller Wahrscheinlichkeit nach nicht mehr besteht

c) wenn diese mit einem unverhältnismäßigen Aufwand verbunden wäre - In diesem Fall hat eine öffentliche Bekanntmachung oder ähnliche Maßnahme zu erfolgen

Sicherheit der Verarbeitung (Art 32)

(1) Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der **Verantwortliche** und der **Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehören:

a) **Pseudonymisierung** und **Verschlüsselung**

b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste müssen auf Dauer sichergestellt werden

c) Verfügbarkeit und Zugang, bei einem physischen oder technischen Zwischenfall müssen rasch wieder hergestellt werden können

d) **Verfahren** zur **regelmäßigen Überprüfung, Bewertung, Evaluierung** der Wirksamkeit der techn. und organisatorischen Maßnahmen

(4) Verantwortliche und Auftragsverarbeiter müssen sicherstellen, dass ihnen unterstellte natürliche Personen nur auf Anweisung des Verantwortlichen personenbezogene Daten verarbeiten.

techn. organisator. Maßnahmen (TOMs)

Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

- Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle**);
- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (**Datenträgerkontrolle**);
- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**);
- Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**)
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (**Zugriffskontrolle**);

techn. organisator. Maßnahmen (TOMs) 2

- Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**);
- Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**);
- Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**);
- Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellung**);
- Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**).

Datenschutz Maßnahmen

- Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Wartung des Verzeichnisses der Verarbeitungstätigkeiten.
- Datenschutzfolgeabschätzungen für geplante Verarbeitungen
- Einbeziehung des Datenschutzbeauftragten (falls vorhanden) in alle Datenvorhaben
- Prozesse zur Wahrung der Betroffenenrechte auf Auskunft, Berichtigung und Löschung.
- Prozesse zur Erfüllung der gesetzlichen Meldepflichten
- Privacy by Design und Privacy by Default

Privacy by Design

Privacy by Design stützt sich auf die Auffassung, dass Datenschutz nicht allein durch die Einhaltung von Rechtsvorschriften gewährleistet werden kann. Vielmehr sollte idealerweise die Gewährleistung des Datenschutzes zum Standardbetriebsmodus jeder Organisation werden.

Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. (Erwägungsgrund 78 DSGVO)

Grundsätze
Privacy by Design

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung
3. Der Datenschutz ist in das Design eingebettet
4. Volle Funktionalität – eine Positivsumme, keine Nullsumme keine falschen Dichotomien wie Datenschutz versus Sicherheit
5. Durchgängige Sicherheit - Schutz während des gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz – Für Offenheit sorgen
7. Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen

Ausgewählte Kapitel

- Fotos - Videoüberwachung
- Pseudonymisierung und Anonymisierung
- Direktwerbung - Spam
- Cookies
- Facebook Pixel

Bildaufnahme (DSG)

§ 12. (1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen.

(2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß § 13 zulässig, wenn

1. sie im lebenswichtigen Interesse einer Person erforderlich ist,
2. die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
3. sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder
4. im Einzelfall **überwiegende berechtigte Interessen des Verantwortlichen** oder eines Dritten bestehen und die **Verhältnismäßigkeit** gegeben ist.

Zulässigkeit der Bildaufnahme (DSG)

(3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 (**überwiegende berechtigte Interessen des Verantwortlichen)** insbesondere dann zulässig, wenn

1. sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,

2. sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist und kein gelinderes geeignetes Mittel zur Verfügung steht, oder

3. sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

Unzulässigkeit der Bildaufnahme (DSG)

(4) Unzulässig ist

1. eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,
2. eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,
3. der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten oder
4. die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

Videoüberwachung

- Für die Videoüberwachungsanlagen ist ein **Hinweis** im Bereich der Videokamera und Informationen für die Hausbewohner erforderlich. Eine Einwilligung ist nicht notwendig.
- Die Videokameras müssen so montiert sein, dass ihre Aufnahmen räumlich **nicht über die Liegenschaft hinausreichen**, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen.
- Die aufgenommenen personenbezogenen Daten sind innerhalb von **72 Stunden zu löschen**, mit Ausnahme von Aufnahmen, die zur Beweissicherung für einen stattgefundenen konkreten Vorfall benötigt werden.
- Es sind dem Risiko des Eingriffs angepasste geeignete **Datensicherheitsmaßnahmen** zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

Urheberrecht (UrhG)

- Werk: Individuelle geistige Leistung erforderlich - im Zweifel: geschütztes Werk
- Schutz beginnt mit Schaffung des Werkes und endet idR 70 Jahre nach Tod des Urhebers
- Rechte des Urhebers entstehen automatisch – keine Registrierung, Kennzeichnung erforderlich
- Bei Fotos: Nicht nur Schutz für urheberrechtliche Werke, sondern jede Art von Foto (z.B. Passfoto, Urlaubsfoto etc.)
- Urheber ist zu nennen
- Zustimmung des Urhebers ist erforderlich
- Fotos dürfen nicht verändert werden

Recht am eigenen Bild im UrhG (§78)

- Persönlichkeitsrecht
- Jeder darf selbst bestimmen, ob er fotografiert wird oder ob diese Bilder veröffentlicht werden
- Ansprüche von Personen aufgrund diverser Abbildungen (Fotos und Videos)
- Bildnisse dürfen idR nur mit vorheriger Einwilligung des Abgebildeten verbreitet bzw. veröffentlicht werden
- Einwilligung schriftlich sinnvoll; auch mündlich und konkludent (stillschweigend) möglich
- Zustimmung erforderlich, sobald Person erkennbar ist (Gesicht, Merkmale, Begleittext etc.)

Zulässigkeit der Bildaufnahme (UhrG)

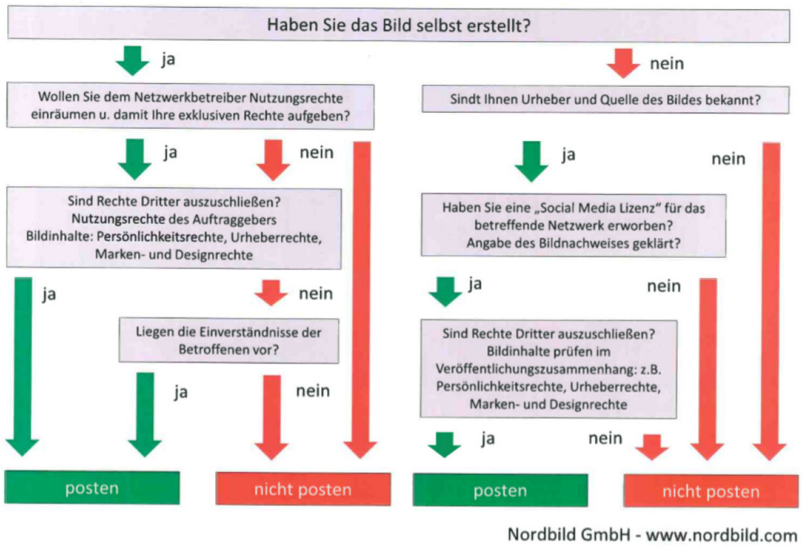
Bei **Personen des öffentlichen Lebens** besteht Veröffentlichungsinteresse oder Informationsinteresse der Allgemeinheit

Interessensabwägung - berechtigtes Interesse vs. Schutz der Persönlichkeit: idR ist davon auszugehen, dass Interessen durch Bildveröffentlichung nicht beeinträchtigt werden

Bei öffentlichen Veranstaltungen, wenn frei zugänglich und mit der Teilnahme damit zu rechnen ist, dass man abgebildet wird

Fotos zur Dokumentation dürfen in diesem Fall idR veröffentlicht werden

Bildrechteprüfung in der Social Media Redaktion: Twitter und Facebook



Nordbild GmbH - www.nordbild.com

Freiheit der Meinungsäußerung und Informationsfreiheit (DSG)

§ 9. (1) Auf die Verarbeitung von personenbezogenen Daten durch Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes im Sinne des Mediengesetzes, zu journalistischen Zwecken finden die Bestimmungen dieses Bundesgesetzes sowie der DSGVO keine Anwendung. Die Datenschutzbehörde hat bei Ausübung ihrer Befugnisse den Schutz des Redaktionsgeheimnisses (§ 31 MedienG) zu beachten.

(2) Soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, finden von der DSGVO mit Ausnahme des Art. 5 (Grundsätze), auf die Verarbeitung, die zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, keine Anwendung. Von den Bestimmungen des DSG ist § 6 (Datengeheimnis) anzuwenden.

Pseudonymisierung

die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können (Art 4 lit 5 DSGVO)

Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. (Erwägungsgrund 26 DSGVO)

Anonymisierung

Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.
(Erwägungsgrund 26 DSGVO)

Anonymisierung (2)

Bescheid der Datenschutzbehörde (DSB)

„Die Entfernung des Personenbezugs („Anonymisierung“) von personenbezogenen Daten kann somit grundsätzlich ein mögliches **Mittel zur Löschung** iSv Art. 4 Z 2 iVm Art. 17 Abs. 1 DSGVO sein. Es muss jedoch sichergestellt werden, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann.“
(GZ: DSB-D123.270/0009-DSB/2018 vom 5.12.2018)

Anonymisierung (3)

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.
Alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, sollten herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind

§ 151 Gewerbeordnung

Die zur Ausübung des **Gewerbes der Adressverlage und Direktmarketingunternehmen** berechtigten Gewerbetreibenden sind berechtigt, für Marketingzwecke Dritter personenbezogene Daten aus öffentlich zugänglichen Informationen, durch Befragung der betroffenen Personen, aus Kunden- und Interessentendateisystemen Dritter oder aus Marketingdateisystemen anderer Adressverlage und Direktmarketingunternehmen zu ermitteln. (unter Beachtung des Grundsatzes der Verhältnismäßigkeit)
Sensible Daten dürfen nur verarbeitet werden, wenn

- ein ausdrückliches Einverständnis dafür vorliegt.
- der Inhaber des Dateisystems gegenüber dem Gewerbetreibenden schriftlich unbedenklich erklärt hat, dass die Betroffenen ausdrücklich einverstanden waren und nur die Stammdaten verwendet werden.

§ 151 Gewerbeordnung

Die zur Ausübung des **Gewerbes der Adressverlage und Direktmarketingunternehmen** berechtigten Gewerbetreibenden sind berechtigt, für Marketingzwecke Dritter personenbezogene Daten aus öffentlich zugänglichen Informationen, durch Befragung der betroffenen Personen, aus Kunden- und Interessentendateisystemen Dritter oder aus Marketingdateisystemen anderer Adressverlage und Direktmarketingunternehmen zu ermitteln. (unter Beachtung des Grundsatzes der Verhältnismäßigkeit)

Sensible Daten dürfen nur verarbeitet werden, wenn

- ein ausdrückliches Einverständnis dafür vorliegt.
- der Inhaber des Dateisystems gegenüber dem Gewerbetreibenden schriftlich unbedenklich erklärt hat, dass die Betroffenen ausdrücklich damit einverstanden waren.

§ 151 Gewerbeordnung - 2

Soweit keine Einwilligung der Betroffenen für die Übermittlung ihrer Daten für Marketingzwecke Dritter vorliegt, dürfen aus einem Kunden- und Interessentendateisystem eines Dritten nur die Daten: Namen, Geschlecht, Titel, akademischer Grad, Anschrift, Geburtsdatum, Berufs-, Branchen- oder Geschäftsbezeichnung und Zugehörigkeit zu diesem Dateisystem, ermittelt werden. Dies nur, sofern der Inhaber des Dateisystems schriftlich unbedenklich erklärt hat, dass die betroffenen Personen über die Möglichkeit informiert wurden, die Übermittlung ihrer Daten für Marketingzwecke Dritter zu untersagen, und dass keine Untersagung erfolgt ist.

Löschungsbegehren sind in jedem Fall innerhalb von einem Monat kostenlos zu entsprechen.

§ 151 Gewerbeordnung - 3

Inhaber von Kunden- und Interessentendateisystemen dürfen personenbezogene Daten aus diesen Dateisystemen an Gewerbetreibende für Marketingzwecke Dritter nur übermitteln und insbesondere auch für Listbroking nur zur Verfügung stellen, wenn sie die betroffenen Personen in geeigneter Weise darüber informiert haben, dass sie die Verarbeitung dieser Daten für Marketingzwecke Dritter untersagen können, und wenn keine Untersagung erfolgt ist.
Aussendungen sind so zu gestalten, dass durch entsprechende Kennzeichnung des ausgesendeten Werbematerials die Identität der Verantwortlichen jener Dateisysteme, mit deren Daten die Werbeaussendung adressiert wurde (Ursprungsdateisysteme), nachvollziehbar ist.

Robinson Listen

Der Fachverband Werbung und Marktkommunikation der WKO hat eine Liste zu führen, in welcher Personen kostenlos einzutragen sind, die die Zustellung von Werbematerial für sich ausschließen wollen. Die Liste ist den österreichischen Adressverlagen und Direktmarketingunternehmen Verfügung zu stellen. Diese dürfen an die in dieser Liste eingetragenen Personen keine adressierten Werbemittel versenden oder verteilen und deren Daten auch nicht vermitteln. E-Mail an werbung@wko.at

Die Telekom-Regulierungsbehörde führt gemäß § 7 des E-Commerce-Gesetzes eine Liste, in die sich alle jene natürlichen und juristischen Personen kostenlos eintragen können, die keine Werbemails erhalten wollen. Dienstanbieter, die E-Mail-Werbung unaufgefordert versenden, müssen diese Liste beachten, indem sie an darin enthaltene Adressen keine Werbemails senden. Diese Liste kann unter folgenden Link abgefragt werden: https://www.rtr.at/de/tk/ECGListe_Web_Abfragen

Spam (§ 107 TKG)

(2) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt.
(3) Ausgenommen im Zusammenhang mit dem Verkauf oder einer Dienstleistung an eigene Kunden und diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und der Empfänger klar und deutlich die Möglichkeit erhalten hat, Zusendungen bei der Daten-Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und
der Empfänger die Zusendung nicht von vornherein, insbesondere durch Eintragung in die Robinson Liste der RTR, abgelehnt hat.

Profiling

Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, **zu bewerten**, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person **zu analysieren oder vorherzusagen** (Art 4 lit 4 DSGVO)

Profiling (2)

Selektionen – das automatisierte Verarbeiten von personenbezogenen Daten um die Personen in Gruppen zusammenzufassen um diesen sie betreffende Angebote oder Informationen zukommen zu lassen.
Die **automatisierte Entscheidungsfindung** unterscheidet sich in ihrem Umfang vom Profiling und kann sich teilweise mit diesem überschneiden oder sich aus diesem ergeben. Bei ausschließlich automatisierter Entscheidungsfindung handelt es sich um die Fähigkeit, Entscheidungen ohne direkte Beteiligung einer Person mithilfe technischer Mittel zu treffen.

Profiling aber wie?

um welche Verarbeitungen (Selektionen, Profiling, Automatisierte Entscheidungsfindung) handelt es sich?

- **Selektionen:** DSGVO. Als Rechtsgrundlage dient die jeweilige Rechtsgrundlage der Verarbeitung woraus selektiert wird.
- **Profiling:** Als Rechtsgrundlage kann die **ausdrückliche Einwilligung** oder das **berechtigte Interesse** dienen. Wichtiges Kriterium ist die Auswirkung vom Profiling auf die betroffenen Personen – bei **sensiblen Daten** ist eine **Datenschutzfolgenabschätzung** notwendig. Auf jeden Fall ist eine **Information** der Betroffenen nötig.

Automatisierte Entscheidungsfindung

Dazu notwendig: (Art 22 DSGVO)

- Information der Betroffenen

Als Rechtsgrundlage

- **ausdrückliche Einwilligung** oder
- sie ist für den Abschluss oder die Erfüllung eines **Vertrags** zwischen der betroffenen Person und dem Verantwortlichen erforderlich.

Maßnahmen um die Rechte der Betroffene zu wahren, wie

- Recht auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung zu ermöglichen

Datenschutzfolgeabschätzung ist durchzuführen

Cookies – e-Privacy RL

Art 5 Abs 3 Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits **im Endgerät eines Teilnehmers oder Nutzers gespeichert sind**, nur gestattet ist, wenn der Betreffende auf der Grundlage von klaren und umfassenden Informationen über die Zwecke der Verarbeitung, seine (ausdrückliche) **Einwilligung** gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikations-netz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Cookies – TKG

§96.(3) Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft sind verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, **welche personenbezogenen Daten er verarbeiten wird**, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine **Einwilligung** dazu erteilt hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck …….(weiter wie RL)

In der dazu gehörigen Strafbestimmung ist allerdings nur die Nicht-Information der Nutzer unter Strafe gestellt, jedoch nicht das Nicht-Einholen einer Einwilligung. (§109 (3) 16)

Cookies – Was ist zu tun ?

Funktionale Cookies

- nur Information darüber (Datenschutzerklärung)

Marketing Cookies

- klare und umfassende Informationen über die Zwecke der Verarbeitung
- ausdrückliche Einwilligung (EU Rechtsvorrang)
- Zustimmung muss zuerst erfolgt sein, erst dann darf Cookie gesetzt werden
- Personen, die diese Zustimmung nicht erteilen, dürfen deshalb keine Nachteile erleiden
- die Zustimmung muss jederzeit und einfach widerrufbar sein -> Cookie ist zu entfernen

Analyse Cookies – Was ist zu tun ?

Analyse Cookies

- Wenn die Daten selbst verarbeitet werden (z.B. Matomo) -> Information
- Wenn die Daten vor Übermittlung anonymisiert werden -> Information
- Wenn dadurch personenbezogene Daten an Dritte übermittelt werden (z.B. Google Analytics) -> Information & ausdrückliche Zustimmung
- bei Personen, die diese Zustimmung nicht erteilen, dürfen keine Cookies gesetzt werden und sie dürfen deshalb keine Nachteile erleiden
- die Zustimmung muss jederzeit und einfach widerrufbar sein -> Cookie ist zu entfernen

Aktivitäten außerhalb von Facebook

Als Aktivitäten außerhalb von Facebook bezeichnet Facebook Informationen zu deinen Interaktionen mit Unternehmen und Organisationen, die letztere mit uns teilen.

Auf Facebook Konto gehen und folgendes klicken:

- Einstellungen
- Deine Facebook Informationen
- Aktivitäten außerhalb von Facebook (Ansehen)
- Deine Aktivitäten außerhalb von Facebook verwalten
- Passwortabfrage

Facebook Off-Activities

Eine Zusammenfassung deiner Aktivitäten, die wir von Unternehmen und Organisationen erhalten. Auch deine Aktivitäten in anderen Apps und auf anderen Websites.

So wurden wir über deine Aktivitäten informiert: Unternehmen und Organisationen teilen deine Aktivitäten mit uns, wenn sie die Business-Tools verwenden. Dazu zählen u. a. das Facebook-Pixel, das Facebook-SDK und Facebook Login.

Aktivitäten von Daten-Dienstleistern und Werbeagenturen: Wenn du einige deiner Aktivitäten nicht wiedererkennst, kann das daran liegen, dass wir sie von Daten-Dienstleistern oder Werbeagenturen erhalten haben. Unternehmen und Organisationen nutzen möglicherweise Drittanbieter, um die Kundeninteraktionen in ihren Apps und auf ihren Websites zu analysieren. Diese Dienstleister oder Agenturen können dann unsere Business Tools verwenden, um uns im Auftrag des Unternehmens oder der Organisation deine Aktivitäten zu übermitteln.

Facebook Off-Activities 2

Anzahl der erhaltenen Interaktionen: Interaktionen sind Handlungen, die du auf einer Website oder in einer App vorgenommen hast. Hier sind einige Beispiele für Interaktionen:

- Das Öffnen einer App
- Das Einloggen in eine App mit Facebook
- Das Ansehen von Inhalten
- Die Suche nach Artikeln
- Das Hinzufügen eines Artikels zum Einkaufswagen
- Der Kauf eines Artikels
- Das Spenden eines Geldbetrags

Facebook Pixel

Das Facebook Pixel ist ein von der Firma Facebook zu Verfügung gestellter code (javascript), der vom Website Betreiber in den Header der Webseite eingefügt wird. Wenn ein Browser diese Seite mit dem Facebook Pixel lädt, wird dessen javascript code ausgeführt. Dadurch lädt der Browser weiteren javascript code (fbevents.js) vom Facebook Server, der ebenfalls vom Browser des Nutzers ausgeführt wird.

Es wird ein Cookie im Browser des Nutzers gesetzt und die Daten des Browsers (IP-Adresse, referrer, browser-Einstellungen, page location, document, und Person, die den Browser benutzt) werden an Facebook übermittelt

Facebook Custom Audiences

Facebook bietet noch weitere Möglichkeiten des Nutzer-trackings und der Erweiterung von Zielgruppen an. Dies wird von Facebook als „Custom Audiences“ und „Lookalike Audiences“ (Erweiterter Abgleich) bezeichnet. Dazu muss der Website Betreiber in das Facebook pixel der jeweiligen Seite eintragen welche Daten bei welchen Aktionen an Facebook geschickt werden sollen. (Button Click Data)

Was Facebook genau mit diesen Daten macht, ist nicht dokumentiert. Seinen Anzeigenkunden bietet Facebook an, sogenannte „Custom Audiences“ zusammenzustellen. Das sind Gruppen von Personen (Facebook Nutzern), denen man als Zielgruppe Werbung schalten kann.

Verwendung Facebook Pixel

- Information der Betroffenen über Funktionalität des Facebook Pixels
- Wenn Button-Click-Data übertragen werden -> Information der Betroffenen welche Daten übertragen werden.
- **ausdrückliche Einwilligung** vor dem Setzen des Cookies und Ausführung des js-codes notwendig. Dazu muss der js-code erweitert werden

Es dürfen auf keinen Fall sensible Daten mittels Button-Click-Data übertragen werden.

Das gelindeste Mittel

Im Artikel 1 (Verfassungsbestimmung) des DSG wird normiert, dass der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf.

Das verpflichtet den Verantwortlichen zu überprüfen ob der gleiche oder ähnliche Effekt nicht auch durch eine datenschutzrechtlich gelindere Maßnahme durchgeführt werden kann.

Danke

Dr. Kurt Einzinger
ke@netelligenz.at