DSGVO

Was tue ich jetzt?

6. Juni 2018

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 Permanent Stakeholders Group of ENISA (European Network and Information Security Agency) (2004-2008, 2017-)
- Cyber Security Forschungsprojekte (CAIS, CIIS,CISA)
- netelligenz – Datenschutz und Cyber Security Beratung
- Externer Datenschutzbeauftragter

Inhalt

- Datenschutz-Grundverordnung (DSGVO)
- Österreich (Grundrecht, DSG, Anpassungen)
- Personenbezogene Daten (Art 9 Daten)
- DSGVO Anforderungen (ausgewählte)
  - Datenverarbeitungsverzeichnis
  - Informationspflichten
  - Datenschutzerklärung – Privacy Policy
  - Auftragsverarbeiter - Mitarbeiterverpflichtung
  - Betroffenenrechte
  - Meldepflichten
  - Datensicherheit - TOMs

Rechtslage Europa

- 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.

Rechtslage Europa (2)

- 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.

Rechtslage Europa (3)

- Neuer Rechtsrahmen der EU
  - Datenschutzgrundverordnung DSGVO
    (seit 25.5.16 in Kraft)
    - gilt ab 25.5.18 in der gesamten Europäischen Union
    - gilt nur wo die EU Kompetenz hat
    - ab 25.5.2018 gilt sie in allen EU Mitgliedsstaaten
  - Richtlinie für Strafverfolgung und justiziellen Bereich (DS-RL 2016/680)
    - umgesetzt im 3.Hauptstück des DSG
  - e-Privacy Richtlinie soll e-Privacy Verordnung werden
    - Lex Specialis zur DSGVO
    - Frühestens Anfang 2019 (dann 1 Jahr Übergangsfrist)

Rechtslage Österreich

- Datenschutzgesetz DSG 2000 (seit 1.1.2000)
- Datenschutzgesetz (DSG) ab: 25.5.2018

  DSG, BGBLA 2017/1/120, 31.7.2017

  - Interministerielle Abstimmung (Jänner bis Mai 2017)
  - Datenschutz-Anpassungsgesetz 2018 (Begutachtung ab 12.5.17)

    Änderung der Verfassungsbestimmungen – neues Gesetz
  - 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 Strafen)
- Datenschutzanpassungsgesetze

DSGVO – Neue Bestimmungen (1)

- gilt nur für natürliche Personen (Art 1 u.a.)
- gilt auch für einen nicht in der Union Niedergelassenen für die Verarbeitung Verantwortlichen (Art 3)
- Recht auf Vergessenwerden (Art 17)
- Recht auf Datenübertragbarkeit (Art 20)
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art 25)
- Auftragsverarbeitungsvereinbarung (Art 28)
- Verzeichnis von Verarbeitungstätigkeiten (Art 30)
- Sicherheit der Verarbeitung (Art 32)
- Meldeverpflichtung (Art 33, 34) Aufsichtsbehörde + Betroffene

DSGVO – Neue Bestimmungen (2)

- Datenschutz-Folgenabschätzung (Art 35)
- Datenschutzbeauftragter (Art 37-39)
- Unabhängige Aufsichtsbehörde (Art 51ff)
- Europäischer Datenschutzausschuss (Art 68ff)
- Recht auf Beschwerde bei Aufsichtsbehörde (Art 77)
- Haftung und Recht auf Schadenersatz (Art 82)
- Verwaltungsrechtliche Sanktionen (Art 83) – wirksam, verhältnismäßig und abschreckend (bis zu 20 Mio € od. 4% vom Jahresumsatz weltweit)
- Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. (ab 25. Mai 2018)

Datenschutz-Grundverordnung (1)

Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten

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

Datenschutz-Grundverordnung (2)

Artikel 6 - Rechtmäßigkeit der Verarbeitung

(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;

Datenschutz-Grundverordnung (3)

Artikel 6 - Rechtmäßigkeit der Verarbeitung

(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.

Übergangsbestimmungen

Erwägungsgrund 171

- Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung (25.5.16) mit ihr in Einklang gebracht werden.
- Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann.

Vorgehensweise bei bestehenden E-Mail Verteilern

- E-Mail Adressen von Kunden, Klienten oder Mitgliedern können weiter verwendet werden. (Da mit ihnen ein Vertrags-Verhältnis besteht)
- E-Mail Adressen, die wir mit Einwilligung des Betroffenen erhalten haben (vor dem 25.5.2018), können auch weiter verwendet werden. (Erwägungsgrund 171 DSGVO) Ein Beleg der Einwilligung (z.B. Eintragungslisten oder Protokolle von Web-Formular-Anmeldung) wäre gut ist aber nicht unbedingt notwendig, solange wir uns der Einwilligung einigermaßen sicher sind.
- Bei E-Mail Adressen unbekannter Herkunft oder die wir nicht von den Betroffenen selbst erhalten haben, sollte um die Einwilligung des Betroffenen nachgefragt werden oder sie sollten aus dem Bestand gelöscht werden

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

(Datenschutzgesetz – DSG)

- Keine neuen Verfassungsbestimmungen
- Nur für natürliche Personen
- Für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtauto-matisierte Verarbeitung personenbezogener Daten
- DSGVO gilt auch außerhalb EU Kompetenz
- Anpassung an DSGVO und Umsetzung der RL 2016/680
- Bestimmungen zur Datenschutzbehörde DSB (§ 18 ff)
- Einrichtung und Aufgaben des Datenschutzrats (§ 14 ff)
- Datenverarbeitungen zu spezifischen Zwecken

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

(Datenschutzgesetz – DSG)

§ 4. Anwendungsbereich und Durchführungsbestimmung

(1) Die Bestimmungen der Verordnung (EU) 2016/679 .... (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, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen.

(2) 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.**

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

(Datenschutzgesetz – DSG)

§ 4 Anwendungsbereich und Durchführungsbestimmung

(4) Bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, ist die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das **vierzehnte Lebensjahr** vollendet hat.

(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**.

(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.

Freiheit der Meinungsäußerung und Informationsfreiheit

§ 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 des Medienunternehmens oder Mediendienstes finden die Bestimmungen dieses Bundesgesetzes sowie von der DSGVO die Kapitel II bis VII und IX keine Anwendung. Die Datenschutzbehörde hat bei Ausübung ihrer Befugnisse gegenüber den im ersten Satz genannten Personen 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 die Kapitel II, mit Ausnahme des Art. 5 (Grundsätze), Kapitel III bis VII Kapitel IX auf die Verarbeitung, die zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, keine Anwendung. Von den Bestimmungen dieses Bundesgesetzes ist in solchen Fällen § 6 (Datengeheimnis) anzuwenden.

Verwarnung durch die Datenschutzbehörde

§ 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.

Zulässigkeit der Bildaufnahme

Ist vorrangig keine Datenschutzproblematik sondern Urheberrecht und Medienrecht

Laut DSG ist auf jeden Fall unzulässig:

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.

Personenbezogene Daten (1)

Begriffsbestimmungen

1. **„personenbezogene Daten“** alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person beziehen**;
2. **Art 9 DSGVO: (sensible) 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

   dürfen nicht verarbeitet werden.

Personenbezogene 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,

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.

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 Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Diese gilt auch für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken.

Der Rat des Datenschutzbeauftragten ist einzuholen

Eine Datenschutz-Folgenabschätzung ist in folgenden Fällen erforderlich:

- Bei systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte 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.

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)

Informationspflichten

- 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

Informationspflichten - 2

- 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.

Informationspflichten - 3

- Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.
- Die Informationen werden unentgeltlich zur Verfügung gestellt.
- Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person 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 den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.
- Bestehen begründete Zweifel an der Identität der natürlichen Person, so können zusätzliche Informationen angefordert werden.

Informationspflichten - 4

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 oder dessen Vertreters

b) Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)

c) Zecke und Rechtsgrundlage 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)

Informationspflichten - 5

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

(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)

Informationspflichten - 6

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.

Informationspflichten - 7

Der Verantwortliche stellt der betroffenen Person die folgenden Informationen zur Verfügung, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

- die Speicherdauer, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die vom Verantwortlichen verfolgt werden;
- das Bestehen eines Rechts auf Auskunft über die betreffenden personenbezogenen Daten sowie der anderen Betroffenenrechte
- wenn die Verarbeitung auf Einwilligung beruht, das Bestehen eines Rechts, diese jederzeit zu widerrufen
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling samt aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Informationspflichten - 8

Der Verantwortliche erteilt die Informationen

- unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch 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 als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung.

Informationspflichten - 9

Die Informationspflicht finden keine Anwendung, wenn und soweit

- die betroffene Person bereits über die Informationen verfügt,
- die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke) oder
- die genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,
- die Erlangung oder Offenlegung durch Rechtsvorschriften, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder
- die personenbezogenen Daten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Informationspflichten - 10

Für Websites:

- Datenschutzerklärung (Privacy Policy) – empfohlen
  - Von allen Seiten erreichbar (wie Impressum)
  - Allgemeine Erklärung, wie von dem Unternehmen personenbezogene Daten verarbeitet werden
  - Hinweis auf Betroffenrechte und Beschwerdemöglichkeit
  - Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten (falls vorhanden)
  - Beschreibung wie die Website mit personenbezogene Daten verfährt
    - Log-Files
    - Cookies
    - Google Analytics etc.
- Informationstext bei allen Formularen, wo personenbezogene Daten erhoben werden – Link zur Datenschutzerklärung

§ 151 Gewerbeordnung

Die zur Ausübung des **Gewerbes der Adressverlage und Direkt-marketingunternehmen** berechtigten Gewerbetreibenden (Gewerbe-treibende) 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 Direkt-marketingunternehmen zu ermitteln, soweit dies unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die Vorbereitung und Durch-führung von Marketingaktionen Dritter einschließlich der Gestaltung und des Versands für Werbemitteln oder das Listbroking erforderlich ist.

Sensible Daten dürfen nur verarbeitet werden, wenn

- ein ausdrückliches Einverständnis zur Verarbeitung für Marketingzwecke Dritter vorliegt.
- bei Daten aus Kunden- und Interessentendateisystemen Dritter, der Inhaber des Dateisystems gegenüber dem Gewerbetreibenden schriftlich unbedenklich erklärt hat, dass die betroffenen Personen mit der Verarbeitung ihrer Daten für Marketingzwecke Dritter ausdrücklich einverstanden waren und nur die Stammdaten verwendet werden

§ 151 Gewerbeordnung - 2

Soweit keine Einwilligung der betroffenen Personen 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 der betroffenen Person zu diesem Kunden- und Interessentendateisystem, ermittelt werden. Dies nur, sofern der Inhaber des Dateisystems schriftlich unbedenklich erklärt hat, dass die betroffenen Personen in geeigneter Weise über die Möglichkeit informiert wurden, die Übermittlung ihrer Daten für Marketingzwecke Dritter zu untersagen, und dass 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.

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

§ 151 Gewerbeordnung - 3

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 mindestens monatlich zu aktualisieren und den Gewerbetreibenden zur Verfügung zu stellen. Diese dürfen an die in dieser Liste eingetragenen Personen keine adressierten Werbemittel versenden oder verteilen und deren Daten auch nicht vermitteln.

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 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

Auftragsverarbeiter Art 28 DSGVO

Der Auftragsverarbeiter muss hinreichend 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 (Dienstgeber) zu melden.

Im besonderen verpflichte ich mich zur sorgfältigen Verwahrung mir anvertrauter Benutzerkennwörter, Passwörter und sonstiger Zugangsberechtigungen.

Meldepflicht (1)

Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(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 (2)

Artikel 34 – Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen

(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

Artikel 32 – Sicherheit der Verarbeitung

(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 technischen und organisatorischen Maßnahmen

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

Sicherheit der Verarbeitung - 2

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**);

Sicherheit der Verarbeitung - 3

- 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-Integration

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

Aufgaben um fürs DSG / DSGVO fit zu sein

- Evaluierung der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten
- Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten
- Anpassung der Datenschutzerklärungen (Websites)
- Texte zur Einhaltung der Informationspflichten
- Geheimhaltungs- und Datenschutzerklärung für Mitarbeiter
- Erstellung eines Prozesses zur Wahrung der Betroffenenrechte auf Auskunft, Berichtigung und Löschung
- Erstellung von Auftragsverarbeitungsvereinbarungen
- Datenschutzrichtlinie (Privacy Policy)
- Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Überprüfung der Sicherheit der Verarbeitungen (Technisch organisatorische Maßnahmen – TOM)

Danke

Dr. Kurt Einzinger
ke@netelligenz.at