Verunsicherung durch die DSGVO: Mythen und Abmahnungen

Prof. Dr. Dirk Heuzeroth

22.06.2018

Hinweis und Haftungsausschluss

- Dieser Vortrag / Foliensatz
  - … gibt einen **Einblick** in die aktuellen datenschutzrechtlichen Vorschriften (hauptsächlich die EU Datenschutzgrundverordnung DSGVO) und damit zusammenhängende weitere Gesetze.
  - … deckt die aktuellen datenschutzrechtlichen Vorschriften und damit zusammenhängende weitere Gesetze **NICHT vollständig** ab.
    - NICHT eingegangen wird z.B. auf
      - die Datenschutzfolgenabschätzung
      - die Bestellung eines Datenschutzbeauftragten
    - Oberflächlich behandelt wird das Thema Auftragsverarbeitung.
  - … stellt **KEINE Rechtsberatung** dar und **ersetzt auch keine Rechtsberatung im Einzelfall**.

Prof. Dr. Dirk Heuzeroth

- Professor für
  Web Development, Software Security and Management
  - Hochschule der Medien Stuttgart
  - heuzeroth@hdm-stuttgart.de
- Freiberuflicher Unternehmensberater
  - Informationssicherheitsmanagementsysteme
  - IT-Sicherheit
  - Datenschutz
- Persönliche Zertifikate:
  - Certified Information Systems Security Professional (CISSP)
  - Certified Ethical Hacker (CEH)
  - Certified ISO/IEC 27001 Lead Implementer (ISO27LI)
  - Certified ISO/IEC 27001 Provisional Auditor (ISO27PA)
  - ITIL v3 Foundation Certified

INHALT

Inhalt

1. Gesetze und Verordnungen
2. Personenbezogene Daten
3. Grundsätze zur Verarbeitung personenbezogender Daten
4. Weitere Verantwortung des für die Verarbeitung Verantwortlichen
   - 4.1 Informationspflichten, Abmahnungen
   - 4.2 Ergreifen technischer und organisatorischer Maßnahmen
   - 4.3 Nachweispflicht und Dokumentationspflicht
   - 4.4 Melde- und Benachrichtigungspflichten
   - 4.5 Haftung und Geldbußen / Strafen
5. Rechte der betroffenen Person
6. Mythen

1.
GESETZE UND VERORDNUNGEN

Datenschutz
(engl. protection of privacy)

- **Datenschutz**:
  - … schützt Persönlichkeitsrechte durch Schutz personenbezogener Daten.
  - … ist ein Grundrecht!
- Grundsätzliche Regel: „**Verbot mit Erlaubnisvorbehalt**“
- Rechtliche Grundlagen:

EU Datenschutzgrundverordnung (DSGVO)

- … wurde am 27.04.2016 erlassen.
- … ist in Kraft seit dem **25.05.2018**.
- Verordnungen der EU gelten im Gegensatz zu Richtlinien unmittelbar, ohne zuvor in nationale Gesetzte überführt zu werden.

Bundesdatenschutzgesetz (BDSG)

- … setzt EU-Recht in nationales Recht um.
- … gilt in der neuen Version seit dem **25.05.2018**.
- … setzt die DSGVO um und legt diese genauer fest.

Landesdatenschutzgesetz (LDSG)

- … ergänzt spezifische Regelungen der Bundesländer.
- … gilt für Behörden und öffentliche Stellen.
- … wird gerade überarbeitet.

Anwendungsbereiche der DSGVO

- Sachlicher Anwendungsbereich (Art. 2 DSGVO)
  - Abs. 1: Die Verordnung gilt für die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten** sowie für die **nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert** werden sollen.
  - Abs. 2 beschreibt **Ausnahmen**, z.B. Buchstabe c:
    - **Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten**
- Räumlicher Anwendungsbereich (Art. 3 DSGVO)
  - Verarbeitung personenbezogener Daten durch **Niederlassung in der Europäischen Union**
  - Verarbeitung von personenbezogener Daten von **Personen, die sich in der Europäischen Union befinden**

2. PERSONENBEZOGENE DATEN

Was sind personenbezogene Daten?

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
  - … solange die Person nicht verstorben ist
  - … sofern die Daten nicht anonymisiert wurden.
- Beispiele:
  - Name
  - Adresse
  - Geburtstag
  - Geburtsort
  - IP-Adresse
  - Cookies
  - Pseudonymisierte personenbezogene Daten
- Beispiele für besondere Kategorien personenbezogener Daten:
  - gesundheitliche Daten (besondere Kategorie nach Artikel 9 DSGVO)
  - ethnische Herkunft (besondere Kategorie nach Artikel 9 DSGVO)
  - Fotos
    - … gelten nicht automatisch als besondere Kategorie, sondern nur dann, wenn es sich um biometrische Daten handelt.

Fragen zu personenbezogenen Daten

- Was kann denn schon schlimmes mit personenbezogenen Daten passieren?

1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/Verträge)
2. Beeinträchtigungen für informationelle Selbstbestimmung
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen
4. Finanzielle Auswirkungen für den/die Betroffenen
5. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen

Wann und wie dürfen personenbezogene Daten verarbeitet werden?

3. GRUNDSÄTZE ZUR VERARBEITUNG PERSONENBEZOGENER DATEN

Grundsätze gemäß Art. 5 DSGVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Nachvollziehbarkeit) (Abs. 1 Buchstabe a)

Zweckbindung (Abs. 1 Buchstabe b):
Für legitime Zwecke, für den Zweck angemessen und erheblich.

Datenminimierung (Abs. 1 Buchstabe c):
Auf das notwendige Maß für den Verarbeitungszweck beschränkt.

Richtigkeit (Abs. 1 Buchstabe d) : Sachlich richtig, vollständig und aktuell. Unverzügliches Löschen oder Berichtigen unrichtiger Daten.

Speicherbegrenzung (Abs. 1 Buchstabe e): Speicherung nur so lange wir für Zwecke erforderlich. Löschkonzept: Löschfristen, Löschregeln (vgl. DIN 66398). Gesetzliche Aufbewahrungsfristen beachten (siehe AO und HGB)!

Integrität und Vertraulichkeit (Abs. 1 Buchst. f): Schutz vor Verlust, Zerstörung, unbefugter oder unrechtmäßiger Verarbeitung → Informations- und IT-Sicherheit!

Rechenschaftspflicht (Abs. 2):
Nachweis der Einhaltung der obigen Grundsätze

Wann ist eine Verarbeitung rechtmäßig?

- Die Antwort gibt Art. 6 Abs. 1 DSGVO:

a) Einwilligung der betroffenen Person für einen oder mehrere Zwecke

b) Erfüllung eines Vertrags mit der betroffenen Person oder Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person

c) Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt.

d) Schützen lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person

e) Wahrnehmung einer Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde

f) Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.
Abs. 2: Dies gilt **nicht** für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Was ist bei Einwilligungen zu beachten?

- Die Antwort gibt Art. 7 DSGVO:

(1) Nachweisbar:
Der Verantwortliche muss nachweisen können, dass die betroffene Person in eingewilligt hat.

(2) Verständlich:
Bei Einwilligung durch schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in **verständlicher** und **leicht zugänglicher Form** in einer **klaren und einfachen Sprache** so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist

(3) Jederzeit widerrufbar

(4) Freiwillig:
Vertrag darf nicht von einer Einwilligung zur Verarbeitung personenbezogener Daten abhängig sein, die für die Erfüllung des Vertrags nicht erforderlich ist.

- Bei Einwilligung zur Werbung Gesetz gegen den unlauteren Wettbewerb (UWG) beachten!

Was ist bei Einwilligungen zu beachten?

- Blüten und Negativbeispiele:
  - https://gdprhallofshame.com/

Wie lässt sich Datenminimierung erreichen?

- Informationelle Gewaltentrennung innerhalb und zwischen verantwortlichen Stellen
- Reduzierung von erfassten Attributen der betroffenen Personen
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen
- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren

Wie lässt sich Richtigkeit / Integrität erreichen?

- Einschränkung von Schreib- und Änderungsrechten
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Krypto-Konzepts
- Dokumentierte Zuweisung von Rechten und Rollen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation
  - der Funktionalität,
  - von Risiken
  - sowie Sicherheitslücken und Nebenwirkungen.

Wie lässt sich Vertraulichkeit erreichen?

- Festlegung eines **Rechte-Rollen-Konzeptes** nach dem Erforderlichkeitsprinzip auf der Basis eines **Identitätsmanagements** und eines **sicheren Authentisierungsverfahrens**.
- **Eingrenzung der zulässigen Personalkräfte** auf solche, die
  - nachprüfbar zuständig (örtlich, fachlich),
  - fachlich befähigt,
  - zuverlässig (ggf. sicherheitsüberprüft)
  - und formal zugelassen sind
  - sowie keine Interessenskonflikte bei der Ausübung aufweisen.
- **Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle**.
- Spezifizierte, **für das Verfahren ausgestattete Umgebungen** (Gebäude, Räume)
- Festlegung und Kontrolle
  - **organisatorischer Abläufe**,
  - **interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.)**.
- **Verschlüsselung** von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (**Kryptokonzept**),
- **Schutz vor äußeren Einflüssen** (Spionage).

Was bedeuten Rechenschaftspflicht und Transparenz?

- **Transparenz** beantwortet die folgenden Fragen:
  - Welche Daten werden für welchen Zweck in einem Verfahren erhoben und verarbeitet
  - Welche Systeme und Prozesse werden dafür genutzt?
  - Wohin fließen die Daten zu welchem Zweck?
  - Wer besitzt die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung?
- Systeme, die personenbezogene Daten verarbeiten, müssen so ausgelegt sein, dass deren gesamte Funktion **nachvollziehbar** ist:
  - Statische Aspekte müssen dokumentiert werden.
  - Dynamische Aspekte müssen protokolliert werden.
  - Protokolle müssen automatisiert ablaufen.

Wie lassen sich Rechenschaftspflicht und Transparenz erfüllen?

- **Dokumentation**
  - … von Verfahren mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Zusammenspiel mit anderen Verfahren,
  - … von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren,
  - … der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen,
  - von Einwilligungen und Widersprüchen,
  - der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts.
- Protokollierung von Zugriffen und Änderungen
- Nachweis der Quellen von Daten (Authentizität)
- Versionierung

4.
WEITERE VERANTWORTUNG DES FÜR DIE VERARBEITUNG VERANTWORTLICHEN

Verantwortungen und Pflichten im Überblick

- Informationspflichten (Transparenz)
- Ergreifen technischer und organisatorischer Maßnahmen
  - Regelmäßige Überprüfung und Aktualisierung der Risikobewertung und Maßnahmen
- Nachweispflicht und Dokumentationspflicht (Rechenschaftspflicht):
  - Nachweis über Einhaltung der DSGVO und des BDSG erbringen.
  - Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Melde- und Benachrichtigungspflichten (Transparenz):
  - Meldung (Art. 33) und Benachrichtigung (Art. 34) von Vorfällen der Verletzung des Schutzes personenbezogener Daten
- Haftung und Geldbußen / Strafen (Art. 82 und 83)

4.1 INFORMATIONSPFLICHTEN

Informationspflichten (1)

- Informationspflichten zum Zeitpunkt der Datenerhebung (Art. 13 DSGVO):
  - Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
  - Ggf. Kontaktdaten des Datenschutzbeauftragten
  - Zwecke der Verarbeitung und Rechtsgrundlage
  - Wenn die Verarbeitung auf Artikel 6 Abs. 1 Buchstabe f DSGVO beruht, das berechtigte Interesse des Verantwortlichen
  - Den Empfänger oder die Kategorien von Empfängern
  - Absicht der Übermittlung in ein Drittland/internationale Organisation sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission
  - Dauer der Datenspeicherung,
  - Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit
  - Recht auf Widerruf einer Einwilligung
  - Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde
  - Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte
  - Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Art. 22).
- Art. 14 Abs. 2 Buchstabe f: Falls Daten nicht bei betroffener Person erhoben wurden, dann Angabe der Quelle.

Informationspflichten (2)

- Für Nutzer von Internet-Seiten muss bekannt gegeben werden,
  - ob und welche Cookies verwendet werden
  - und ob die Nutzer der Seiten „ge-trackt“ werden.
    - z.B. Google Analytics
- Bei Übermittlung von Daten an Dienstleister ist eine **Auftragsverarbeitungsvereinbarung** erforderlich!

- Die Angaben dieser und der vorangegangenen Folie sind Teil der **Datenschutzerklärung**!
  - Achtung: Abmahngefahr mittels UWG …

Gesetz gegen den unlauteren Wettbewerb (UWG) (1)

- § 1 Zweck:
  - Dieses Gesetz dient dem **Schutz der Mitbewerber, der Verbraucherinnen und Verbraucher sowie der sonstigen Marktteilnehmer vor unlauteren geschäftlichen Handlungen**.
  - Es schützt zugleich das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb.
- § 3 Verbot unlauterer geschäftlicher Handlungen
- § 5a Irreführung durch Unterlassung
  - Abs. 2: Unlauter handelt, wer im konkreten Fall unter Berücksichtigung aller Umstände dem Verbraucher eine **wesentliche Information vorenthält** …
  - Abs. 4: Als wesentlich im Sinne des Absatzes 2 gelten auch Informationen, die dem Verbraucher auf Grund **unionsrechtlicher Verordnungen oder nach Rechtsvorschriften zur Umsetzung unionsrechtlicher Richtlinien** für kommerzielle Kommunikation einschließlich Werbung und Marketing nicht vorenthalten werden dürfen.
- § 7 Unzumutbare Belästigungen (Werbung)

Gesetz gegen den unlauteren Wettbewerb (UWG) (2)

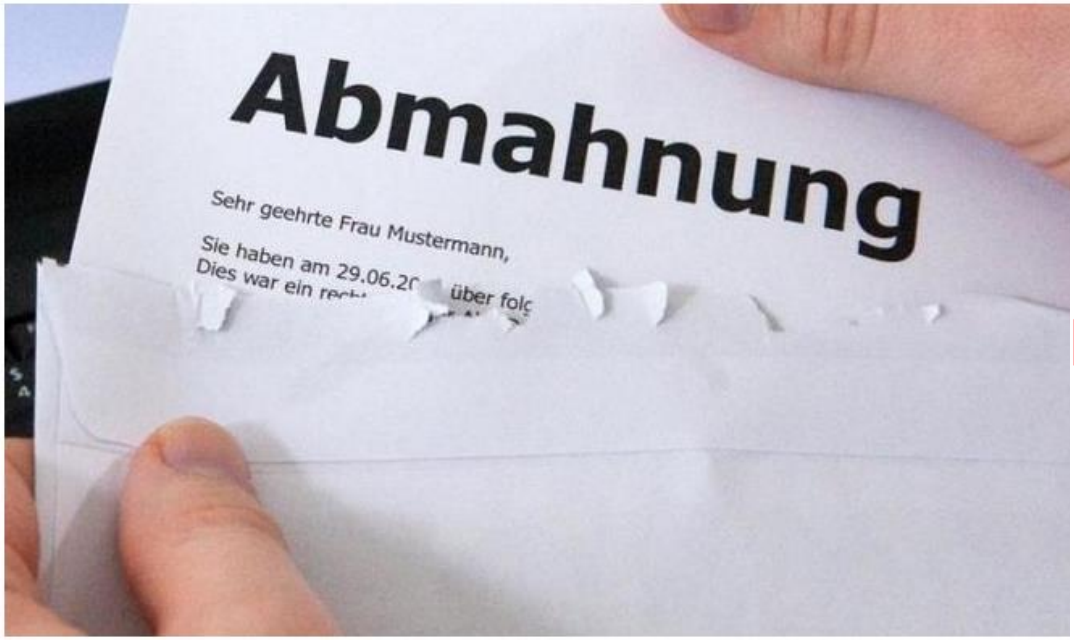
- § 8 Beseitigung und Unterlassung
  - Abs. 1: Wer eine nach § 3 oder § 7 unzulässige geschäftliche Handlung vornimmt, kann auf Beseitigung und bei Wiederholungsgefahr auf **Unterlassung** in Anspruch genommen werden …
- § 12 Anspruchdurchsetzung, Veröffentlichungsbefugnis, Streitwertminderung
  - Abs. 1: Die zur Geltendmachung eines Unterlassungsanspruchs Berechtigten sollen den Schuldner vor der Einleitung eines gerichtlichen Verfahrens **abmahnen** und ihm Gelegenheit geben, den Streit durch Abgabe einer mit einer angemessenen Vertragsstrafe bewehrten Unterlassungsverpflichtung beizulegen. Soweit die Abmahnung berechtigt ist, kann der **Ersatz der erforderlichen Aufwendungen** verlangt werden.

Unklarheiten in Bezug auf Abmahnungen

DSGVO: Die Abmahn-Maschinerie ist angelaufen

30.05.2018 14:55 Uhr – Holger Bleich

vorlesen



(Bild: dpa, Andrea Warnecke/Illustration)

Die ersten Rechtsanwaltskanzleien berichten von Abmahnungen wegen angeblicher Verstöße gegen die neue EU-Datenschutz-Grundverordnung (DSGVO). Dabei geht es um Beanstandungen von Unternehmen zu Websites von Mitbewerbern.

Rechtsanwalt Matthias Hechler aus Schwäbisch Gmünd etwa erklärt, dass er am 25. Mai bereits drei Abmahnungen in den Händen hielt, in denen Verstöße gegen die DSGVO geahndet würden. In zwei Fällen sei die Verwendung von Google Analytics ohne Opt-In-Möglichkeit gerügt worden, in einem Fall das Setzen von Cookies. Generell ginge es um die angebliche Fehlerhaftigkeit der vorhandenen Datenschutzerklärungen. Die Fristen zur Abgabe einer Unterlassungserklärung betrugen laut Hechler bei allen drei Abmahnungen kurze zwei Werktage.

Quelle: https://www.heise.de/newsticker/meldung/DSGVO-Die-Abmahn-Maschinerie-ist-angelaufen-4061044.html?xing_share=news

Unklarheiten in Bezug auf Abmahnungen

- Fit für die DSGVO (PDF)
- DSGVO: Last-Minute-Hilfe
- Folterfragebogen im Selbsttest
- Datenschützer fühlen sich unvorbereitet
- Kommentar: Auf die Großen zugeschnitten

Fehlende Datenschutzerklärung

Rechtsanwalt Alexander Bräuer von der Kanzlei Weiß&Partner aus Esslingen berichtet, dass ein Unternehmen ebenfalls am 25. Mai von einem vorgeblichen Mitbewerber abgemahnt worden sei. Die Abmahnung wurde demnach vom Augsburger Rechtsanwalt Orhan Aykac ausgesprochen. Grund der kostenpflichtigen Rechtsbelehrung sei eine gänzlich fehlende Datenschutzerklärung. Dies wäre allerdings auch schon vor der DSGVO-Wirksamkeit rechtswidrig gewesen.

Bemerkenswert: Anwalt Aykac nennt Bräuer zufolge einen Gegenstandswert von hohen 7.500 Euro. Dieser setze sich zusammen "aus dem Jahreswert der Kosten für die vollständige und ordnungsgemäße Umsetzung der DSGVO", habe Aykac erklärt. Dieser Gegenstandswert würde Abmahngebühren von mehr als 700 Euro bedeuten.

Quelle: https://www.heise.de/newsticker/meldung/DSGVO-Die-Abmahn-Maschinerie-ist-angelaufen-4061044.html?xing_share=news

Unklarheiten in Bezug auf Abmahnungen

Unklare Rechtslage

Die genannten Abmahnungen leiten ihre Berechtigung aus dem Gesetz gegen den unlauteren Wettbewerb (UWG) ab. Bislang ist unklar, ob Unternehmen ihre Konkurrenten wegen Verstößen gegen Datenschutzrecht aus wettbewerbsrechtlichen Gründen abmahnen oder verklagen dürfen. In Deutschland gab es hierzu auch vor der DSGVO keine einheitliche Rechsprechung. Das OLG Hamburg beispielsweise bejahte 2013 diese Frage, Das Kammergericht Berlin dagegen 2011 nicht. (hob)

Quelle: https://www.heise.de/newsticker/meldung/DSGVO-Die-Abmahn-Maschinerie-ist-angelaufen-4061044.html?xing_share=news

4.2 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Technische und organisatorische Maßnahmen (1)

- Artikel 24 DSGVO verlangt:
  - **Geeignete technische und organisatorische** Maßnahmen, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.
    - **Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.**
  - **Geeignete Datenschutzvorkehrungen**
    - … sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht.
  - Nachweis der Erfüllung der Pflichten des Verantwortlichen, z.B. durch
    - Einhaltung der **genehmigten Verhaltensregeln** gemäß Artikel 40
    - oder eines **genehmigten Zertifizierungsverfahrens** gemäß Artikel 42
      - z.B. Datenschutzsiegel

Technische und organisatorische Maßnahmen (2)

Art. 32 DSGVO (**Sicherheit der Verarbeitung**), Abs. 1 verlangt

- **… geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**
  - a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
  - b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste** im Zusammenhang mit der Verarbeitung **auf Dauer sicherzustellen**;
  - c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen **bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen**;
  - d) ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung.

Technische und organisatorische Maßnahmen (3)

Konsequenz:

- **Informationssicherheitsmanagementsystem (ISMS) ist zwingend erforderlich.**

ISMS Standards und Normen sind z.B.:

- **ISO 27001 bzw. die ISO 27000er Normenreihe**
- **BSI Grundschutz**
- **VdS 3473**
- **ISIS12**

4.3 NACHWEIS- UND DOKUMENTATIONSPFLICHT

Nachweise über die Einhaltung der DSGVO: Verzeichnis von Verarbeitungstätigkeiten

- Artikel 30 DSGVO, Abs. 1 **für Verantwortlichen (datenerhebende Stelle)**:

  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**;

  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 bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen 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 Maßnahmen gemäß** Artikel 32 Absatz 1.

Nachweise über die Einhaltung der DSGVO: Verzeichnis von Verarbeitungstätigkeiten

- Artikel 30 DSGVO, Abs. 2 **für Auftragsverarbeiter**:

  Inhalt des Verzeichnisses::

  a) den **Namen und die Kontaktdaten des Auftragsverarbeiters** oder der Auftragsverarbeiter und **jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist**, sowie gegebenenfalls des **Vertreters des Verantwortlichen oder des Auftragsverarbeiters** und eines etwaigen **Datenschutzbeauftragten**;

  b) die **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden;

  c) 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 bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

  d) wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1.

Nachweise über die Einhaltung der DS-GVO: Verzeichnis von Verarbeitungstätigkeiten

- Artikel 30 DSGVO
  - Das Verzeichnis von Verarbeitungstätigkeiten ist

(3) **… schriftlich zu führen**, z.B. in einem **elektronischen Format**

(4) **… der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen**.

(5) Die in den Absätzen 1 und 2 genannten Pflichten **gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn**

- … die von ihnen vorgenommene 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 gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

4.4
MELDE- UND BENACHRICHTIGUNGS-PFLICHTEN

Meldepflicht:
Welche Vorfälle sind wann zu melden?

- Artikel 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 gemäß Artikel 55 **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 des Schutzes personenbezogener Daten** bekannt wird, **meldet er diese dem Verantwortlichen unverzüglich**.

Meldepflicht:
Was muss die Meldung enthalten?

- Artikel 33 DSGVO:

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

- **eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze**;
- den **Namen und die Kontaktdaten des Datenschutzbeauftragten** oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine **Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten**
- eine **Beschreibung der** von dem Verantwortlichen **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Meldepflicht:
Schrittweise Lieferung und Dokumentation

- Artikel 33 DSGVO:

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung **schrittweise zur Verfügung stellen**.

(5) Der Verantwortliche **dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.** Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

Benachrichtigungspflicht: Benachrichtigung betroffener Personen

- Art. 34:
  - Abs. 1: **Unverzügliche Benachrichtigung** der von einer **Verletzung des Schutzes personenbezogener Daten** betroffenen Person **bei voraussichtlich hohem Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen.
  - Abs. 2: Beschreibung der Verletzung in klarer und einfacher Sprache.
  - Abs. 3: **Ausnahmen** von der Benachrichtigungspflicht:
    a) Bei Anwendung geeigneter technische und organisatorischer Maßnahmen, z.B. Verschlüsselung.
    b) Bei Treffen von Maßnahmen, die sicherstellen, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht.
    c) Bei unverhältnismäßig hohem Aufwand.
      - Ersatzmaßnahme:
        Öffentliche Bekanntmachung oder ähnliche Maßnahme.
  - Abs. 4: Nachholung der Benachrichtigung möglich

4.5
HAFTUNG
UND GELDBUßEN / STRAFEN

Wer haftet?

- Artikel 82 DSGVO:

(1) **Jede Person**, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, **hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter**.

(2) **Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden**, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.
Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) **Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.**

Wie hoch sind die Geldbußen?

- Artikel 83 DSGVO:

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 **in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist**.

(4) Bei einigen Verstößen können **Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist**.

(5) Bei anderen Verstößen können sogar **Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.**

(6) Bei **Nichtbefolgung einer Anweisung der Aufsichtsbehörde** gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von **bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist..**

Wie hoch sind die Geldbußen?

- Artikel 83 DSGVO:

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 **in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist**.

(4) Bei einigen Verstößen können **Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist**.

(5) Bei anderen Verstößen können sogar **Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des**

ABER:

- § 27 LDSG neu:
  Gegen öffentliche Stellen dürfen keine Geldbußen verhängt werden.
- § 28 LDSG neu:
  Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe für Mitarbeiter.

Quelle: https://beteiligungsportal.baden-wuerttemberg.de/fileadmin/redaktion/beteiligungsportal/IM/171214_Gesetzentwurf-Neufassung-Landesdatenschutzgesetz.pdf

5.
RECHTE DER BETROFFENEN PERSON

Welche Rechte haben betroffene Personen?

Art. 15: Auskunftsrecht der betroffenen Person

Art. 16: Recht auf Berichtigung

Art. 17: Recht auf Löschung („Recht auf Vergessenwerden“)

Art. 18: Recht auf Einschränkung der Verarbeitung

Art. 19: Offenlegung aller Empfänger gegenüber der betroffenen Person

Art. 20: Recht auf Datenübertragbarkeit

Art. 21: Widerspruchsrecht

Art. 22: Recht, nicht ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden. Ausnahmen: Abschluss oder Erfüllung eines Vertrages mit der Person, Rechtsvorschriften, Ausdrückliche Einwilligung der betroffenen Person.

Wann und wie müssen die Rechte der betroffenen Person erfüllt werden?

- Die Antwort gibt Art. 12 DSGVO:
  - **In präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache.**
  - **Unverzüglich**, in jedem Fall aber **innerhalb eines Monats**.
    - **Fristverlängerung um 2 Monate möglich** unter Berücksichtigung der Komplexität und Anzahl der Anfragen.

- Erinnerung:
  - Die Aufklärung über die Rechte der betroffenen Person muss auch in der **Datenschutzerklärung** erfolgen!

6. MYTHEN

Quelle:
https://www.impulse.de/recht-steuern/rechtsratgeber/dsgvo-mythen/7305128.html

Mythos Nr. 1

- **Der 25. Mai 2018 ist noch nicht relevant, weil dann erst die einzelnen Landesgesetze verhandelt werden.**
  - Falsch!
  - Die DSGVO gilt als Verordnung seit Mai 2016, am 25.05.2018 endete die zweijährige Übergangszeit.

Mythos Nr. 2

- **Für jeden Verstoß gegen die DSGVO müssen 20 Millionen Euro oder vier Prozent des Jahresumsatzes Strafe bezahlt werden.**
  - Falsch!
  - Das sind lediglich die Maximalstrafen.
  - Die Aufsichtsbehörden haben bei der Verhängung von Strafen aber Spielraum.

Mythos Nr. 3

- **Jeder muss jetzt einen Datenschutzbeauftragten haben**
  - Falsch!
  - Einen Datenschutzbeauftragten muss ein Unternehmen nur bestellen, **wenn mindestens zehn Mitarbeiter als Kerntätigkeit persönliche Daten verarbeiten**.
    - Allerdings zählt hierbei jeder Mitarbeiter mit – auch wenn er nur einmal pro Woche personenbezogene Daten bearbeitet oder in Teilzeit angestellt ist.
  - **Unabhängig von der Mitarbeiterzahl** braucht ein Unternehmen auch dann einen Datenschutzbeauftragten, wenn **besonders sensible Daten** verarbeitet werden, für die eine **Datenschutz-Folgeabschätzung** notwendig ist.
  - Und auch für **Unternehmen, die personenbezogene Daten an Dritte übermitteln** – wie beim klassischen Adresshandel – oder sie zu Markt- und Meinungsforschungszwecken verarbeiten, ist ein Datenschutzbeauftragter Pflicht.
  - **Behörde oder öffentlichen Stellen** müssen auch einen Datenschutzbeauftragten benennen.
  - Allerdings muss man einen Datenschutzbeauftragten nicht in Vollzeit beschäftigen, es kann sich dabei auch um einen **externen Dienstleister** ☺ handeln.

Mythos Nr. 4

- **Jede Datenerfassung bedarf einer Einwilligung**
  - Falsch!
  - Art. 6 Abs. 1 DSGVO erlaubt neben der Einwilligung auch andere Bedingungen für eine rechtmäßige Verarbeitung z.B.
    - Erfüllung eines Vertrages mit der betroffenen Person
    - Rechtliche Verpflichtung
    - Berechtigtes Interesse
  - Beispiele:
    - Wer auf einer Messe eine Visitenkarte bekommt mit der Bitte, ein Angebot zu senden, der benötigt für den Versand eines solchen keine schriftliche Einwilligungserklärung.
    - Für Kontaktformulare auf Websites benötigt man keine Einwilligungserklärung – sie dienen in der Regel nämlich der Vertragsanbahnung.

Mythos Nr. 5

- **Die DSGVO verbietet die Datenübermittlung in die USA**
  - Falsch!
  - Was die Auftragsverarbeitung betrifft, erlaubt die DSGVO nun sogar, dass diese auch außerhalb der EU stattfinden darf.
  - Anforderungen der DSGVO an eine Datenübermittlung ins Nicht-EU-Ausland wie die USA:
    - **Garantie, dass das Datenschutzniveau dort dem der Europäischen Union entspricht.**
    - Um das nachzuweisen, gibt es verschiedene Möglichkeiten:
      - eine Zertifizierung unter dem **EU-US-Privacy-Shield**
        - zertifizierte Firmen finden sich auf der Privacy-Shield Liste (http://www.privacyshield.gov/list)
      - oder ein **Datenschutz-Zertifikat** nach DSGVO, das Firmen künftig erwerben können.

Mythos Nr. 6

- **Unternehmen dürfen nur noch per verschlüsselter E-Mail kommunizieren**
  - Falsch!
  - Die DSGVO sieht **keinen Zwang zur Verschlüsselung** vor, **auch wenn diese sicher in vielen Fällen sinnvoll ist**.
  - Ob der Versender eine E-Mail verschlüsseln muss, **hängt vom Schutzbedarf** der übertragenen Daten ab.
    - Nur wenn es um Daten geht, die nach Artikel 9 Absatz 1 der DSGVO einen **sehr hohen Schutzbedarf** haben, ist eine **Verschlüsselung** notwendig.
    - Dies sind beispielsweise
      - Gesundheitsdaten
      - Daten zur sexuellen Orientierung
      - oder biometrische Daten.

Mythos Nr. 7

- **Wer Menschen fotografiert, muss immer eine schriftliche Genehmigung von allen einholen**
  - Falsch!
  - Digital erstellte **Foto- und Videoaufnahmen zählen tatsächlich als Verarbeitung von personenbezogenen Daten** und die derzeitige Rechtslage ist unsicher.
  - Experten sind allerdings der Meinung, dass wer das **Kunsturhebergesetz** und die recht strenge Rechtsprechung **beachtet**, in der Regel davon ausgehen kann, dass damit auch die Vorgaben der DSGVO erfüllt werden.
  - Politiker, Juristen und Datenschützer sind sich einig:
    - **Wichtige Grundrechte wie Kunst- und Pressefreiheit sollen durch die Datenschutz-Grundverordnung nicht ausgehebelt werden.**

Mythos Nr. 8

- **Alle alten Adresslisten müssen gelöscht werden**
  - Falsch!
  - Wer bisher personenbezogene Daten erfasst hat
    und sich dabei **an die Rechtslage gehalten** hat
    und auch **nachweisen kann, dass er eine Einwilligung zur Verarbeitung der Daten hat**,
    der kann alte Adressen weiter nutzen.

Mythos Nr. 9

- **Die DSGVO verbietet es, personenbezogene Daten in einer Cloud zu speichern**
  - Falsch!
  - Personenbezogene Daten dürfen weiterhin in einer Cloud gespeichert werden – allerdings muss man mit dem Cloud-Betreiber einen **Vertrag zur Auftragsverarbeitung** schließen und für den gelten strengere Vorgaben als bisher.
  - Der Cloud-Anbieter muss **hinreichende Garantien** dafür bieten, dass er **geeignete technische und organisatorische Maßnahmen** getroffen hat, die sicherstellen, dass die **Datenverarbeitung im Einklang mit den Anforderungen der DSGVO** erfolgt und dass die **Rechte der Betroffenen gewährleistet** werden.

QUELLEN

Quellen

- DSGVO (EU Verordnung 2016/679)
  - Originalquelle:
    - https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
  - im Internet aufbereitet: https://dsgvo-gesetz.de/
- BDSG (neu) im Internet aufbereitet:
  - https://dsgvo-gesetz.de/bdsg-neu/
  - https://dejure.org/gesetze/BDSG
- LDSG
  - bisher: https://dejure.org/gesetze/LDSG
  - Entwurf für Neufassung:
    - https://beteiligungsportal.baden-wuerttemberg.de/fileadmin/redaktion/beteiligungsportal/IM/171214_Gesetzentwurf-Neufassung-Landesdatenschutzgesetz.pdf
- heise Artikel über Abmahn-Machinerie:
  - https://www.heise.de/newsticker/meldung/DSGVO-Die-Abmahn-Maschinerie-ist-angelaufen-4061044.html?xing_share=news
- 9 Mythen rund um die Datenschutz-Grundverordnung:
  - https://www.impulse.de/recht-steuern/rechtsratgeber/dsgvo-mythen/7305128.html
- GDPR Hall of Shame:
  - https://gdprhallofshame.com/
- Logo auf Titelbild von Alice Schlotterbeck