BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

Webseiten datenschutzkonform gestalten

Aktuelle Regelungen zu Cookies & Co.

Webinar IHK Würzburg-Schweinfurt am 28.07.2025

Carolin Loy

Bayerisches Landesamt für Datenschutzaufsicht

Funktionsweise des Internets

- Durch Eingabe einer URL (Uniform Resource Locator) im Browser wird eine Webseite aufgerufen, dies stellt einen sog. Request dar
- Technisch: Anfrage des Nutzers an den Server auf dem die Inhalte der Webseite gespeichert sind
- Hierzu wird die URL über einen DNS- Server in eine IP- Adresse umgewandelt
- Anfrage enthält die Anforderung alle Datenpakete zum Aufruf zu übermitteln

+ verschiedene Informationen des Nutzers: IP-Adresse, Spracheinstellungen, Browser..

-> erforderlich für korrekte Darstellung

- Datenpakete werden an den Browser geschickt, verarbeitet -> Webseite erscheint
- Sofern Drittdienste eingebunden sind werden nicht nur Inhalte vom Webserver der Webseite, sondern auch von Dritten geladen
  - Schriftarten, Videos, Sicherheitstools, Chatbots, Banner, Social Media Plug-Ins

Cookies

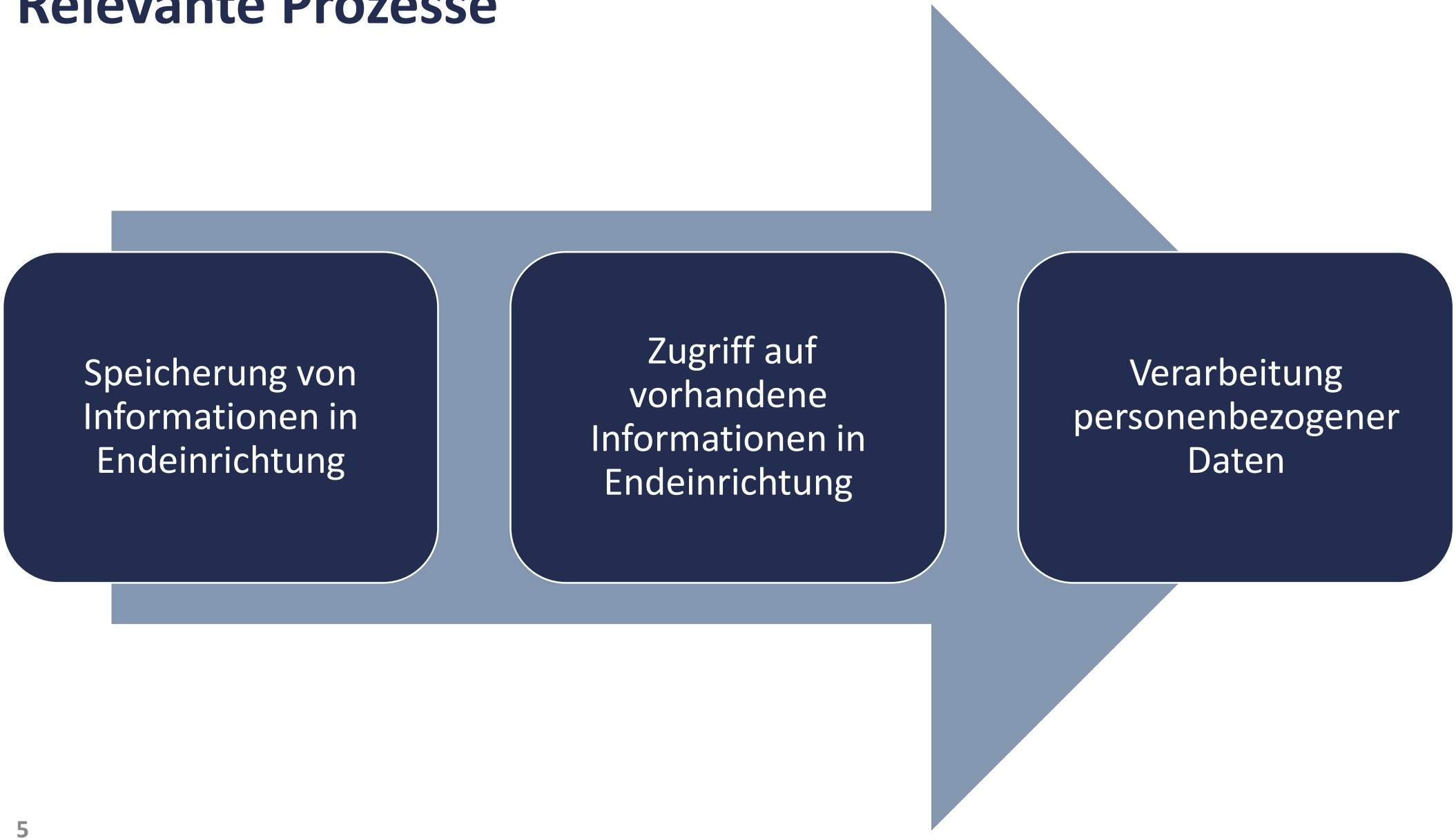
- Kleine Textdateien, die auf dem Gerät des Nutzers gespeichert werden
- Unterschiedliche Lebensdauer:
  - Session- Cookies (z.B. Warenkorb, Speichern von Voreinstellungen)
  - Persistente Cookies (Tracking)
- Dient der Wiedererkennung des Nutzers
- Cookies bestehen aus einem Namen (Key) und einem Wert (Value)
- Wert kann eindeutig sein – Wiedererkennung eines konkreten Nutzers
- Unterscheidung First- Party und Third- Party- Cookies

Tracking

- Nicht definiert: **Nachverfolgung des Nutzers**
- Vor allem zu Werbezwecken
- Nutzungsverhalten:
  - Aufgerufene Webseite (sog. Clickstream)
  - Verwendetes Gerät
  - Standort, Zeitpunkt und Dauer der Nutzung
- **Geräte- und Webseitenübergreifend** möglich
- Verknüpfung von Merkmalen oder Interessen zu einem **Nutzungsprofil**

- Aber auch Bereich **Cybersecurity**: z.B. Vermeidung von DDOS- Attacken
- Betrugsprävention
- **Optimierung / Sicherstellung der Funktionsfähigkeit einer Webseite**

Relevante Prozesse



Personenbezogene Daten bei der Onlinenutzung

- Anwendbarkeit der DS-GVO – Personenbezug?
- Kann eine natürlich Person unmittelbar identifiziert werden?
- Kann die Identifizierung durch Zusatzwissen erreicht werden?
- Alle Mittel berücksichtigen, die „nach allgemeinem Ermessen wahrscheinlich“ genutzt werden
- Kosten, Zeitaufwand, Technologie…
- Objektiver oder subjektiver Ansatz? -> EuGH C-319/22 vom 09.11.2023
- IP Adresse – EuGH C-582/14 vom 19.10.2016 „Breyer“
- EuG, 08.01.2025 - T-354/22 (subj. Ansatz + obj. Elemente)

- Benutzerkennungen, Cookie-IDs, Standortdaten, Profildaten eines Online- Accounts, E-Mail Adresse, Werbe-IDs, Mac- Adressen
- IP- Adressen- EuGH C-582/14 vom 19.10.2016 „Breyer“

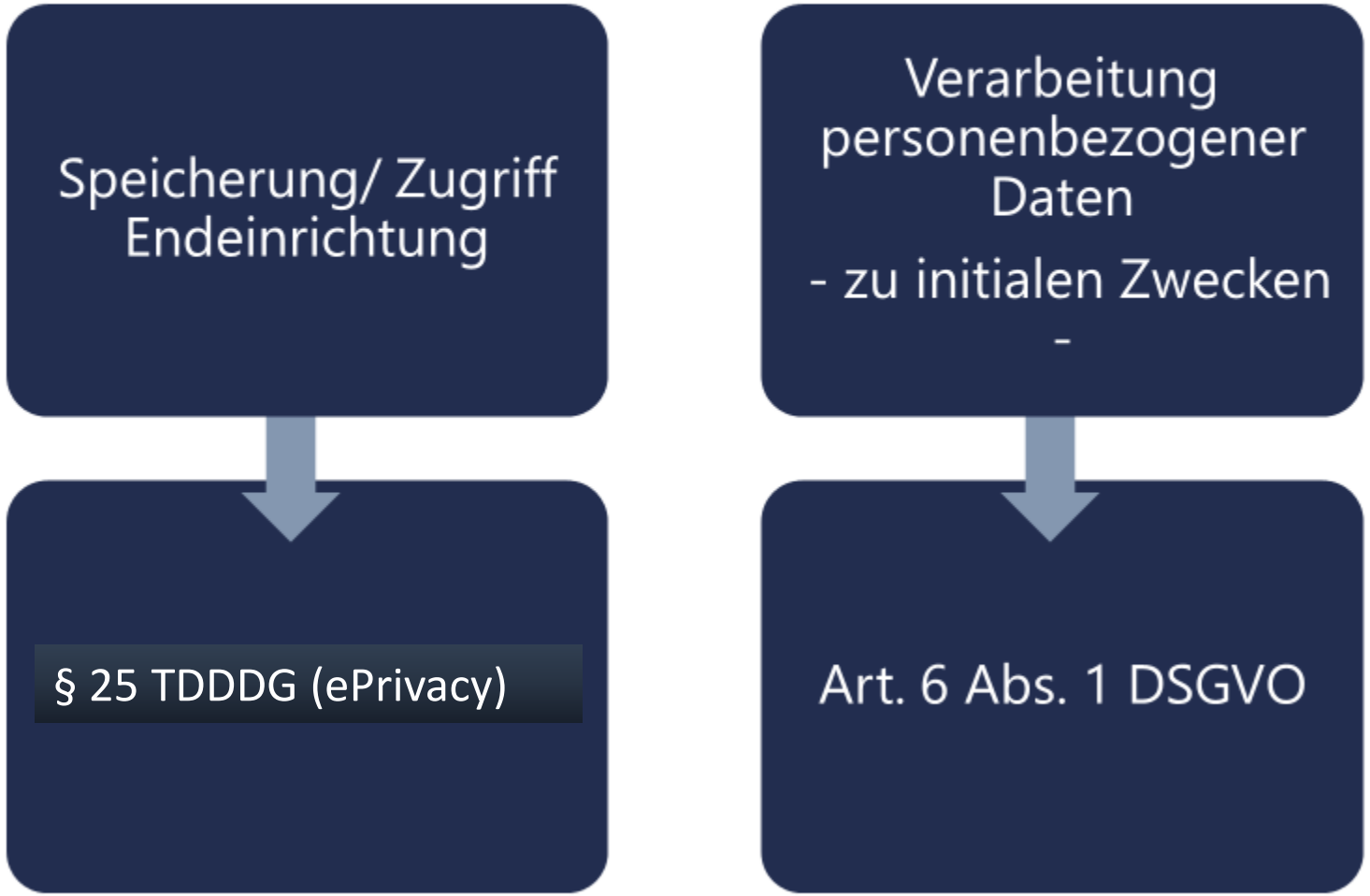
Rechtlicher Rahmen für Datenschutz auf Webseiten

- Zweistufige Prüfung:
  - Zugriff auf die Endeinrichtung
  - Verarbeitung personenbezogener Daten

- Telekommunikation – Digitale- Dienste- Datenschutzgesetz + DS-GVO

- Orientierungshilfe Digitale Dienste 2024
  (https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf)
- https://www.lda.bayern.de/media/checkliste/baylda_checkliste_handel_solo.pdf
- https://www.lda.bayern.de/de/faq.html

Rechtsrahmen



Sanktionen

- Bußgelder
  - § 28 Abs. 1 Nr. 13 TDDDG Owi- Tatbestand bei Verstoß gegen § 25 Abs. 1 S. 1 TDDDG
  - § 28 Abs. 2 TDDDG -> 300.000 €
  - ABER: Daneben auch Verstöße gegen die DSGVO möglich

- Zuständigkeit
  - BfDI für TK- Dienste, öffentliche Stellen des Bundes § 29 TDDDG
  - im Übrigen die Landesaufsichtsbehörden § 1 Abs. 1 Nr. 8 TDDDG
  - BNetzA §30 TDDDG im Hinblick auf Teil 2 Datenschutz und Schutz der Privatsphäre in der Telekommunikation -> Sofern nicht BfDI

Adressat des § 25 TDDDG

Betreiber einer Webseite oder App sind auch für die Prozesse verantwortlich, die durch die technische Gestaltung der Webseite/ App verursacht werden.

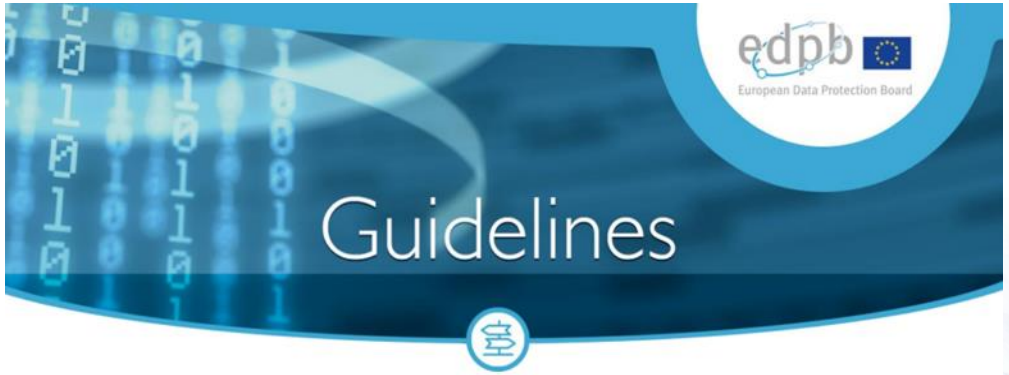
Die Einhaltung der Rechtmäßigkeitsvoraussetzungen muss nachgewiesen werden können.

§ 25 TDDDG - Anwendungsbereich

- „Information“ nicht pbD
- Endgerät eine Nutzers
- ‘storage’ /‘gaining of access’

- Speicherung von Informationen
- Kein zeitliches Minimum

- Zugriff auf Informationen
- Aktiv?
- Anweisung Informationen zu senden



Guidelines 2/2023 on Technical Scope of Art. 5(3)
of ePrivacy Directive

Version 2.0

Adopted on 7 October 2024

§ 25 TDDDG - Anwendungsbereich

- Cookies
- Fingerprinting
- Pixel / Tracking- Links
- Mac- oder IP-Adressen
- Authentifizierungstoken
- Session- Identifier
- Ableitungen von Informationen von lokalen Anwendungen
- Local Storage / WebSQL
- Malware

Einwilligungspflicht
Ja oder Nein?!
„Ob“?

Ausnahmen

- Die Einwilligung nach Absatz 1 ist **nicht** erforderlich,

  wenn der **alleinige Zweck** der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen **die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist** oder

  wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen **unbedingt erforderlich** ist, damit der Anbieter eines Telemediendienstes einen **vom Nutzer ausdrücklich gewünschten Telemediendienst** zur Verfügung stellen kann.

Ausnahmen

- Ausnahme Abs. 2 Nr. 2:

„unbedingt erforderlich“

- dem Wortlaut nach nicht zwingend technisch (aber: Gesetzesbegründung)
- Erw. Gr. 66 der Richtlinie 2009/136/EG „technische Speicherung“
- Sicht des Nutzers / Nutzererwartung (genereller Bezug auf den Nutzer)

„vom Nutzer ausdrücklich gewünscht“

- durch aktive Handlung des Nutzers
- Dienst im Sinne von einzelnen Funktionen i.d.R. nicht Gesamtangebot

Ausnahmen

- Virtuelles „Hausrecht“
- Aufruf einer Website nicht Nutzerwunsch nach gesamten Angebot
- Nutzerwunsch im Regelfall nur nach Kenntnis
- „Mehrzweck-Cookies“
- Einwilligung zentral über Consent- Banner od. an konkreter Stelle
- Pflichtenkollision

- Problempunkte: Reichweitenmessung und wirtschaftliche Erforderlichkeit

Reichweitenmessung

- Was ist Reichweitenmessung?

- Grundsätzlich nie (technisch) unbedingt erforderlich

  -> z.B. mittels Logfile- Analyse

- Unter engen Voraussetzungen möglich

  - kein berechtigtes Interesse -> nachfolgende Verarbeitung
  - Fehlerfreie Auslieferung der Website = Nutzerwunsch
  - Navigationsprobleme

Reichweitenmessung

- Die CNIL führt zu den Voraussetzungen in Art. 5 des Beschlusses Nr. 2019-093 vom 4. Juli 2019 zur Annahme von Leitlinien für die Anwendung von Artikel 82 des Gesetzes vom 6. Januar 1978 in der geänderten Fassung auf Lese- oder Schreibvorgänge auf dem Endgerät eines Nutzers (insbesondere auf Cookies und andere Tracker), abrufbar unter: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038783337 aus:
- sie müssen vom Herausgeber der Website oder von seinem Subunternehmer umgesetzt werden;
- Die Person muss vor ihrer Durchführung informiert werden;
- Es muss die Möglichkeit geben, über einen Widerspruchsmechanismus Einspruch einzulegen, der auf allen Terminals, Betriebssystemen, Anwendungen und Webbrowsern problemlos verwendet werden kann. Auf dem Gerät, von dem aus die Person widersprochen hat, darf kein Lese- oder Schreibvorgang stattfinden;
- Der Zweck des Systems muss sich auf (i) die Messung des Publikums der angesehenen Inhalte beschränken, um die Bewertung der veröffentlichten Inhalte und der Ergonomie der Website oder Anwendung zu ermöglichen, (ii) die Segmentierung des Publikums der Website in Kohorten, um die Wirksamkeit der redaktionellen Entscheidungen zu bewerten, ohne dass dies zu einer Ausrichtung auf eine einzelne Person führt, und (iii) die dynamische Änderung einer Website auf globaler Weise.
- Die erhobenen personenbezogenen Daten dürfen nicht mit anderen Verarbeitungsvorgängen (z.B. Kundendateien oder Statistiken über Besuche auf anderen Seiten) zusammengeführt oder an Dritte übermittelt werden. Der Einsatz von Trackern sollte auch strikt auf die Erstellung anonymer Statistiken beschränkt sein. Ihr Geltungsbereich muss auf einen einzigen Herausgeber einer Website oder mobilen Anwendung beschränkt sein und darf nicht die Verfolgung des Surfverhaltens der Person ermöglichen, die verschiedene Anwendungen verwendet oder auf verschiedenen Websites surft.
- Die Verwendung der IP-Adresse zur Geolokalisierung des Internetnutzers darf keine genaueren Informationen als die Stadt liefern. Die erhobene IP-Adresse muss auch gelöscht oder anonymisiert werden, sobald die Geolokalisierung durchgeführt wurde;
- Die bei diesen Behandlungen verwendeten Tracer dürfen eine Lebensdauer von nicht mehr als dreizehn Monaten haben und diese Dauer darf bei neuen Besuchen nicht automatisch verlängert werden. Die über die Tracker gesammelten Informationen müssen für einen Zeitraum von maximal fünfundzwanzig Monaten aufbewahrt werden.

Wirksame Einwilligung „Wie“?

Wirksame Einwilligung

Weiter ohne Einwilligung auf 1. Ebene

- Zunächst: Muss eine Wahl getroffen werden? Kann eine Einwilligung eingeholt werden?
- Einheitlichkeit zwischen den europäischen Aufsichtsbehörden*
- Gesetzgeberische Struktur
- Einwilligung über vorausgewählte Optionen (EuGH - C-673/17 - Planet49)
- Freiwilligkeit – Gibt es eine Option zum Ablehnen? Soll der Nutzer von der freien Wahl abgehalten werden?* Mehraufwand?
- Unmissverständliche, eindeutige, für den bestimmten Fall abgegebene Willenserklärung
- Grundsatz von Treu und Glauben
- Ebenso einfach wie die Erteilung einer Einwilligung vgl. Art. 7 Abs. 3 S. 1, 4 DS-GVO
- Einzelfallbetrachtung bei der Ausgestaltung

*Délibération n° 2020-092 « recommandation » unter 28 (https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf) oder „Ablehnen von Cookies muss so leicht sein, wie diese zu akzeptieren“ (https://www.cnil.fr/fr/cookies-une-vingtaineorganismes-mis-en-demeure)
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegend

*BGH GRUR 2020, 891, Rn. 37 – Cookie-Einwilligung II

Gestaltung

- Buttons müssen nicht identisch sein -> Aber Wahlmöglichkeiten erkennbar!
- Eindeutige und unmissverständliche Handlung möglich?
- Grundsatz von Treu und Glauben (Farben, Kontrast, Stellung bewusst „irreführend“ gewählt?)
- in der Regel Einzelfallbetrachtung und Gesamtschau
- Verstoß = keine Einwilligung?

  -> Folge: Sämtliche Prozesse auf Grundlage der Einwilligung rechtswidrig!

Information

- Angabe der Rechtsgrundlage -> § 25 Abs. 1 TDDDG / Art. 6 Abs. 1 lit. a) DS-GVO
  -> Im Übrigen in die Datenschutzerklärung (bei pbD)
  -> Consent- Banner: Nur die Dienste die eine Einwilligung benötigen
  -> Empfehlung: Übersicht über alle Cookies mit RGL

- Verweis § 25 Abs. 1 S. 2 TDDDG auf Informationspflichten der DS-GVO
- Konkret „Cookies“ benennen / Verarbeitungstätigkeiten sofern pbD

- Zwecke darstellen
  - Kategorien alleine sind nicht ausreichend
  -> Es muss ersichtlich sein, welche Dienste zu welcher Kategorie gehören (Ausklappmenüs)
  - Zweckbündelung erlaubt, sofern nicht wesentlich unterschiedlich

Der Nutzer muss verstehen in was er einwilligt und was das bedeutet!

- Vor allem bei der Schaltfläche „Alle akzeptieren“

Information

- Mehrebenenansatz --> Einwilligung aber erst auf der Ebene möglich auf der konkrete Informationen zu den einzelnen Zwecken gegeben werden
- Hinweis auf das Widerrufsrecht
- Verlinkung zu vollständiger Datenschutzerklärung
- Speicherdauer
- Übersichtliche Gestaltung -> keine Vorgaben wie viele Layer ein Consent- Banner haben darf

- **Der Nutzer muss verstehen in was er einwilligt und was das bedeutet!**

Andere Rechtsgrundlagen?

Vertrag – Art. 6 Abs. 1 lit. b)

- Zur Erfüllung des Vertrags „erforderlich“
  -> reine Nützlichkeit reicht nicht aus

- Klar erkennbar
- Zweckbindung -> keine Weiterentwicklung / Optimierung

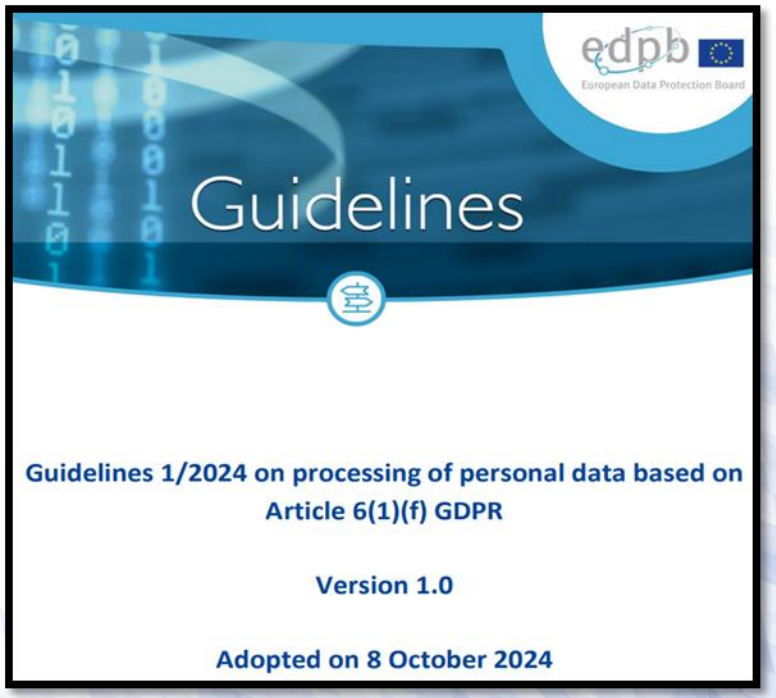
- Online- Werbung grds. nicht auch wenn zur Finanzierung der Webseite

- Bezahlen mit Daten vs. „Consent or pay“
- Guidelines EDSA (2/2019 abrufbar unter:
  https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf

Berechtigtes Interesse – Art. 6 Abs. 1 lit. f)

- Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR
  https:/www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

- Drei- Stufen – Test:
  - Legitimer Zweck
  - Notwendig
  - Interessensabwägung



Berechtigtes Interesse – Art. 6 Abs. 1 lit. f)

Interessensabwägung:

- Vernünftige Erwartungen der betroffenen Personen und Vorhersehbarkeit/ Transparenz
- Interventionsmöglichkeiten der betroffenen Personen – überobligatorisch
- Verkettung von Daten möglich?
- Beteiligte Akteuere – je höher die Anzahl, desto höher das Risiko?
- Dauer der Beobachtung
- Kreis der Betroffenen – Minderjährige?!
- Datenkategorien
- Umfang der Datenverarbeitung

Datenschutzerklärung

- Grundsatz der Transparenz Art. 5 Abs. 1 lit. a DS-GVO
- Nutzer soll Datenverarbeitungen nachvollziehen können
- Art. 13 DS-GVO Informationspflicht (Verarbeitung pbD bereits bei Aufruf – Logfiles/ Protokolldaten)
- Art. 12 Abs. 1 S. 1 DS-GVO: „leicht zugänglich“ – max. 2 Klicks, nicht hinter dem Banner
- nur Informationstext – keine Einwilligung – kein „Akzeptieren“ erforderlich
- Inhalt:
  - individuell – je nach Datenverarbeitungen
  - Mindestinhalt: Art. 13 DS-GVO
  - Bereitstellung der Webseite und Verarbeitung von Log- Files
  - Verarbeitungen von Informationen aus Onlinebestellungen /Kontaktformular
  - Einsatz von Tools zur Reichweitenmessung
  - Einbindung von Diensten Dritter (Kartendienste, Schriftarten, Social Media Plug-Ins, Zahlungsabwicklung…)

Betroffenenrechte

- Auskunft Art. 15 DSGVO
- Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht (edpb_guidelines_202201_data_subject_rights_access_v2_de.pdf)
- Berichtigung Art. 16 DSGVO
- Löschung/ „Recht auf Vergessenwerden“ Art. 17 DSGVO
- Datenübertragbarkeit Art. 20 DSGVO
- Widerspruch Art. 21 DSGVO

Fragen?

Carolin Loy

Bayerisches Landesamt für Datenschutzaufsicht

-

Promenade 18, 91522 Ansbach
https://www.lda.bayern.de