Inhaltsverzeichnis

1 Änderungshistorie

Datum/Version	Änderer	Änderung
20191010	ssch	Erstellung
20191025	ssch	Anpassungen

2 Anzuwendendes Recht

Bei der Umsetzung dieser Anleitung sind folgende Rechtsvorschriften anzuwenden:

- Datenschutzgrundverordnung (DSGVO)
- ePrivacy-Verordnung (ePVO) – aktueller Stand
- Telemediengesetz (TMG)
- Rechtsprechungen
- Orientierungshilfen, Stellungnahmen der Datenschutz-Aufsichtsbehörden

Bitte beachten Sie, dass es sich bei dieser Anleitung um eine allgemeingültige Anleitung handelt. Für die genaue Bewertung einer Website ist stets eine Einzelfallbetrachtung notwendig.

3 Verarbeitungen ohne Einwilligungspflicht

Technisch unbedingt notwendige Cookies

- Die durch den Verantwortlichen selbst und technisch unbedingt notwendig sind. Zum Beispiel die Funktion eines Warenkorbs oder die Einstellung einer Schriftgröße. [1]

Benötigte Session-Cookies

- Ein Session Cookie speichert Informationen, die Onlineaktivitäten einer einzelnen Browser-Sitzung zuordnen. Diese werden beim Schließen des Browsers wieder gelöscht. [2]

4 Verarbeitungen mit Einwilligungspflicht

Alle Verarbeitungen, die nicht technisch notwendig sind, z. B.:

- Lokale Tracking-/Analysetools (z. B. Matomo). Seit Urteil des EuGHs vom 01.10.19 dürfen auch lokal eingebundene Trackingdienste (die keine Verbindung zu Dritten aufbauen) nicht mehr ohne rechtskräftige Einwilligung betrieben werden.
- Web-Fonts (wie z. B. Google WebFonts)
- Tracking-/Analysetools-Anbieter (wie z. B. Google Analytics)
- Affiliate-Dienste (Weiterleitungen auf Partnerlinks und Erfolgsmessung)
- Remarketing-Dienste (ein „Zurückholen" eines Interessierten mittels Werbeanzeigen)
- Retargeting-Dienste (ein „Zurückholen" eines Interessierten i. d. R. mit Mails oder Newslettern)
- Pixel-Tracking (kleine Grafiken die beim Ansurfen der Seite eine Verbindung zu einem separaten Server aufbauen)
- Skalierbare zentrale Messverfahren (SZM)
- Plugins (wie z. B. Facebook Like-Button)
- Video-Einbindungen (wie z. B. YouTube)
- Karten/Maps-Einbindungen (wie z. B. Google Maps)
- Browser-Fingerprinting [3]
- Google AdWords

5 Einholen von Einwilligungen durch ein Cookie-Banner (insb. für Drittanbieterdienste)

- Beim erstmaligen Besuch der Webseite ist ein Cookie-Banner einzusetzen

- Der Cookie-Banner muss eine Übersicht über die einwilligungsbedürftigen Verarbeitungsvorgänge (Cookies) unter Nennung der beteiligten Akteure und deren Funktion enthalten
- Das Cookie-Banner darf die Datenschutzerklärung und das Impressum nicht verdecken
- Eine Einwilligung in eine Gruppe von Dritt-Anbieter-Cookies kann durch ein Opt-In eingeholt werden. Allerdings muss der Besucher die Möglichkeit haben, granular nur einzelne Cookies der Gruppe mittels Opt-In auszuwählen (z. B. in einem „Detail-Bereich"). Ein „Aktiviert" darf in beiden Fällen nicht voreingestellt sein, es ist eine aktive Handlung des Besuchers [z. B. Haken setzen oder Klick auf Schaltfläche etc.] nötig.
- Es muss eine Möglichkeit zum Widerruf / zur Deaktivierung geben
- Bevor eine Einwilligung abgegeben wurde müssen die Cookies gesperrt / blockiert sein, erst mit der Einwilligung ist die Aktivierung der Cookies durchzuführen
- Das Ergebnis der Auswahl / Einwilligung / Widerspruchs ist ohne Verwendung einer User-ID o.ä. vom Verantwortlichen (z. B. durch ein Cookie ohne Personenbezug) auf dem Endgerät des Benutzers zu speichern

6 Allgemeine Anforderungen an Einwilligungen

6.1 Vorab
- Es ist zu gewährleisten, dass die Trackingskripte (z.B. google analytics, matomo) bis zur Abgabe der Einwilligung blockiert sind

6.2 Freiwilligkeit
- Die Webseite muss auch ohne Einwilligung besuchbar sein. Es darf kein Opt-Out bestehen.

6.3 Informiertheit
- Dem Nutzer sind alle relevanten Informationen (wie bspw. Zweck der Verarbeitung, Betreiber, Funktionsdauer der Cookies, ob Dritte Zugriff auf die Cookies erhalten können [4]) zur Verfügung zu stellen. Ein Cookie-Banner muss eine Verlinkung zur Datenschutzerklärung aufweisen.

6.4 Granular
- Es darf keine allgemeingültige Erklärung eingeholt werden. Dem Nutzer muss die Gelegenheit zu einer granularen Information gegeben werden, für welche Verarbeitungen und für welche Anbieter die Einwilligung gegeben wird.

6.5 Explizit
- Die Einwilligung ist explizit, durch einen Klick (Opt-In) einzuholen. Es darf kein Opt-Out-Verfahren eingesetzt werden. Ferner muss es eine Schaltfläche für ein Ablehnen der Einwilligung geben [5]

6.6 (Einfach) Widerrufbar
- Die Einwilligung muss genauso einfach zu widerrufen sein, wie die Einwilligung

6.7 Dokumentiert
- Die Einwilligung ist dokumentiert und nachweisbar einzuholen. Es reicht aus, wenn auf dem Endgerät des Besuchers das Ergebnis für oder gegen eine Einwilligung gespeichert wird (z. B. durch ein Cookie ohne Personenbezug).

6.8 Transparent
- Über die Verarbeitung ist transparent zu informieren (Datenschutzerklärung)

7 Informationen

7.1 Information in einem Cookie-Banner:
- Welche Informationen mit Cookies gespeichert werden
- Zu welchem Zweck diese Informationen gespeichert werden
- Ob Dritte Zugriff auf die Cookies haben (Third-Party-Cookies)
- Einen Link zur Datenschutzerklärung
- Dauer der Speicherung / Gültigkeit der Cookies

7.2 Information durch eine Datenschutzerklärung

Folgende Punkte müssen in der Datenschutzerklärung beachtet werden:

- Allgemeine Pflichtangaben aus Artikel 12 ff. DSGVO:
  - Namen, Kontaktdaten des Verantwortlichen (ggf. Vertreter),
  - Kontaktdaten des Datenschutzbeauftragten,
  - Bestehen der Rechte der Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit, ggf. Widerruf der Einwilligung, Beschwerderecht bei einer Aufsichtsbehörde,
- Pflichtangaben aus Artikel 13 ff. DSGVO die separat für jede Verarbeitung angegeben werden müssen:
  - Zwecke und Rechtsgrundlagen der Verarbeitungen,
  - ggf. die berechtigten Interessen, die verfolgt werden,
  - ggf. die Empfänger oder Kategorien von Empfängern,
  - ggf. Übermittlung in ein Drittland (Angemessenheitsbeschluss, Verweis auf geeignete Garantien, Möglichkeit zur Kopie dieser Garantien),
  - die Dauer (oder die Kriterien für die Festlegung der Dauer) der Speicherung,
  - ob die Bereitstellung gesetzlich oder vertraglich vorgeschrieben oder erforderlich ist und Folgen bei Nichtbereitstellung
  - das Bestehen einer automatisierten Entscheidungsfindung einsch. Profiling
- Die o.g. Angaben sind für jedes Verfahren aufzuführen: Eigene Cookies, Server-Log-Dateien, Kontaktformular, Registrierungen, Kommentarfunktionen, Übermittlungen für Online-Shopping, Social-Media-Tools und -Plugins, Analyse-Tools und Werbung, Newsletter, Plugins und iFrames (z. B. Videos), Web-Schriftarten, Karten-Einbindungen, Captcha-Dienste, Übermittlungen zu Ticket-/Kundenanfragesysteme, Partnerprogramme, Zahlungsdienstleister, Bewerbungsformulare
- Sollten allerdings bestimmte Verfahren nicht zum Einsatz kommen, so sollten diese auch nicht Erwähnung finden, da dies gegen eine transparente Information verstößt.
- Einfache Erreichbarkeit auf der gesamten Webseite
- Einfache Auffindbarkeit durch deutliche Kennzeichnung (nicht im / unterm Impressum versteckt, eigene Verlinkung oder „Impressum/Datenschutz")

8 IT-Sicherheit[1]

- Verfügt Ihre Internetseite über eine ausreichende https-Verschlüsselung? Ausreichend sind nicht veraltete TLS-Protokolle und/oder ein unsicherer Algorithmus.
- Werden dem Benutzer bei Registrierung (oder Änderung) Hinweise für ein ausreichend starkes Passwort gegeben? Wird eine Mindestlänge des Passworts vorgegeben? (Empfehlung 12 Zeichen)
- Wird eine Maximallänge des Passworts vorgegeben? (Empfehlung keine Beschränkung / 100 oder mehr Zeichen)
- Wird ein starkes Passwort (nach akt. Passwortrichtlinien) erzwungen oder können auch schwache Passwörter (12345678, abcdefgh, etc.) verwendet werden? Sind die Komplexitätsanforderungen an ein Passwort vorgegeben (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen nötig)?
- Wird der Nutzer über die Passwortstärke informiert? Anzeige durch farbigen Balken etc
- Ist eine Zwei-Faktor-Authentifizierung möglich?
- Wird nach der Registrierung eine Bestätigungs-E-Mail an den Nutzer versandt, um die Registrierung abzuschließen?
- Wird der Nutzer vor Phishing-Angriffen gewarnt bzw. ausreichend darüber informiert?

[1] Nicht alle hier aufgeführten Sicherheitsmaßnahmen müssen für jede Homepage relevant sein, z.B. Kennwortvorgaben

- Wird der Nutzer über fehlgeschlagene Logins informiert bzw. ob sich über fremde Geräte eingeloggt wurde?
- Wird bei Änderung des Passworts das aktuelle Passwort abgefragt?
- Erhält der Nutzer eine E-Mail mit Information, dass sein Passwort geändert wurde?
- Wird ein sicheres Verfahren für die Funktion "Passwort vergessen" verwendet? (Kein Klartext des neuen Passwortes in E-Mail verwenden)
- Kann der Nutzer Informationen und Hilfe erhalten bezüglich eines "Account-Diebstahls"?
- Wird auf Ihrer Internetseite auch der Schutz von anonymisierten Daten gewahrt? Z. B. Geo-ID's
- Sind die technischen und organisatorischen Maßnahmen angemessen?
- Werden kritische Daten verschlüsselt gespeichert? Dies ist z.B. für gespeicherte Kennworte zwingend notwendig (MD5 nicht ausreichend).

9 Auftragsverarbeitungen gem. Art. 28 DSGVO

Folgend erfolgt eine zusammenfassende Übersicht über mögliche Auftragsverarbeiter:

- Anbieter von Tracking-Tools
- Webhoster
- Dienstleister für E-Mail-Versand (Newsletter / Kontaktformular / Bewerberformular, etc.)
- Sonstige Dienstleister, denen im Kontext des Webseitenbetriebs personenbezogene Daten im Auftrag übermittelt werden

10 Außerhalb der EU

Außerhalb der EU (/EWR) bestehen Möglichkeiten zur Übermittlung durch

- wenn ein Angemessenheitsbeschluss der EU für diesen Staat vorliegt
- geeignete Garantien
  - Standarddatenschutzklauseln,
  - Binding Corporate Rules
  - Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus
  - Einzeln ausgehandelte Vertragsklauseln
- Ausnahmen für bestimmte Fälle
  - Einwilligung
  - Erforderlichkeit zur Vertragserfüllung
  - Wichtige Gründe des öffentlichen Interesses
  - Verfolgung von Rechtsansprüchen
  - Schutz lebenswichtiger Interessen
  - Wahrung zwingender berechtigter Interessen

11 Gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO

Beim Einsatz von einigen Diensten kann eine Gemeinsame Verantwortlichkeit vorliegen. Diese bedarf ebenfalls der „Schriftform“:

- Facebook-Fanpages

12 Weitere Anforderungen

Folgende Maßnahmen sollten unternommen werden, um den Datenschutz zu erhöhen und eine rechtskonforme Verarbeitung zu gewährleiten

12.1 Google Analytics

- Aktivierung der IP-Anonymisierung [6] Anleitung
- Anpassung der Speicherdauer auf das Minimum
  - Anleitung:
  - Für diese Schritte benötigen Sie Bearbeitungsrechte

- Melden Sie sich bei GA an (https://analytics.google.com/analytics/web/provision/?authuser=0#/provision)
- Klicken Sie auf den Link Verwaltung (Zahnrad unten links)
- Es öffnet sich ein auf der rechten Seite dreigeteiltes Fenster
- Dort in dem Reiter „Property" befindet sich an vierter Stelle die Schaltfläche „Tracking Info"
- Klicken Sie auf „Tracking Info".
- Klicken Sie auf den weiteren Unterpunkt „Datenaufbewahrung"
- Auf der rechten Seite können Sie nun unter dem Stichpunkt „Aufbewahrung von Nutzer- und Ereignisdaten" 14 Monate mittels Drop-Down-Menü einstellen
- Klicken Sie auf Speichern

- Abschluss der Datenverarbeitungsbedingungen
  - Anleitung:
  - Für diese Schritte benötigen Sie Bearbeitungsrechte
  - Melden Sie sich bei GA an (https://analytics.google.com/analytics/web/provision/?authuser=0#/provision)
  - Klicken Sie auf den Link Verwaltung (Zahnrad unten links)
  - Es öffnet sich ein auf der rechten Seite dreigeteiltes Fenster
  - Dort in dem Reiter „Account" befindet sich an erster Stelle die Schaltfläche „Account Settings"
  - Klicken Sie auf „Zusatz zur Datenverarbeitung anzeigen" oder "Zusatz anzeigen"
  - Klicken Sie dann auf Akzeptieren
  - Klicken Sie nun auf Speichern.
  - Klicken Sie anschließend wieder im Reiter Account Settings
  - Ganz unten befindet sich die Schaltfläche „DPA Details verwalten"; dort klicken Sie bitte
  - Es öffnet sich ein neues Fenster
  - Bei „Legal entities" sollte Ihr Unternehmen vermerkt sein, wenn nicht tragen Sie es bitte nach. (Rechts oben mittels Bleistiftsymbol)
  - Im Punkt „Contacts" können Sie nun Kontaktpersonen eintragen. (Rechts oben mittels Plussymbol)
  - Dort tragen eine Kontaktperson („Primary contact") und einen „Data protection officer" ein

12.2 Tracking-Anbieter
- Benutzer-IDs sollten pseudonymisiert sein
- Auf nicht genutzte gehashte / verschlüsselte Daten sollte verzichtet werden
- Transaktions-IDs sollte eine alphanummerische Datenbankkennung aufweisen

12.3 Web-Fonts
- Lokale Einbindung der Schriftarten auf dem eigenen Web-Server mit Sicherstellung, dass keine Verbindungen zu den Servern von Google bestehen.

12.4 YouTube
- YouTube-Videos sollten nur im sog. erweitertem Datenschutzmodus auf der Webseite eingebettet werden. Die angesteuerte Server-Adresse lautet alsdann https://www.youtube-nocookie.com. [7] Anleitung

12.5 Respektieren von „Do Not Track"
- Die Browser-Einstellungen des Besuchers (z. B. "Do not track") sind zu berücksichtigen

12.6 Google Maps
- Google-Maps-Einbindungen sind nur mit einer Einwilligung einzubinden. Diese kann durch eine Klick-Lösung innerhalb der Karte geschehen oder durch einen Cookie-Banner.

12.7 Anforderungen bei Einsatz eines Kontaktformulars
- Bei Erhebung von personenbezogenen Daten über ein Kontaktformular ist eine Transportverschlüsselung (SSL-Zertifikat / https-Verschlüsselung) notwendig
- Versand der Kontakt-Mail über SMTP mit TLS
- Datensparsamkeit: Keine unnötigen Pflichtangaben erzwingen

- Zwischen Formular und Senden-Button muss ein Hinweis mit Link zur Datenschutzerklärung vorhanden sein. Bspw.: „Ich habe die Datenschutzerklärung zur Kenntnis genommen und bestätige dies mit dem Absenden der Nachricht. Ich stimme zu, dass meine Angaben und Daten zur Beantwortung meiner Anfrage elektronisch erhoben und gespeichert werden. Die Einwilligung kann ich jederzeit für die Zukunft widerrufen."
- Ggf. Erweiterung des Hinweises ähnlich: „Die angegeben Daten werden zur Beantwortung der Kontaktanfrage verwendet und anschließend entweder gelöscht oder zur weiteren Bearbeitung von Anfragen / zur Auftragsabwicklung gespeichert. Dabei gelten gesetzliche Aufbewahrungsfristen."
- Entsprechende Vereinbarungen zur Auftragsverarbeitung abschließen (Hoster, ggf. E-Mail-Marketing-Service)

12.8 Anforderungen bei Versand eines Newsletters / Registrierung zum Newsletter

- Folgende Anforderungen bestehen bei Einsatz eines Newsletter-Services:
- Der Versand eines Newsletter benötigt eine Einwilligung, welche nachweisbar dokumentiert werden muss (Double Opt-In-Lösung mit Speicherung der IP-Adresse, Name und Uhrzeit)
- In jedem Newsletter muss auf das Widerrufsrecht hingewiesen werden
- Aufklärung über Art, Umfang und Zwecke der Erhebung und Verwendung der personenbezogenen Daten, über die Verarbeitung der Daten in allgemein verständlicher Form in der Datenschutzerklärung
- Entsprechende Vereinbarungen zur Auftragsverarbeitung abschließen (Bei Einsatz von Dienstleistern zum Newsletter- / E-Mail-Versand)

1 https://www.baden-wuerttemberg.datenschutz.de/zum-einsatz-von-cookies-und-cookie-bannern-was-gilt-es-bei-einwilligungen-zu-tun-eugh-urteil-planet49/
2 https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
3 https://ec.europa.eu/newsroom/article29/news-overview.cfm
4 http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=2101905
5 http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=2101905
6 https://support.google.com/analytics/answer/2763052?hl=de
7 https://support.google.com/youtube/answer/171780?hl=de