Die Datenschutz-Checkliste

Open Source Checkliste um datenschutz-relevante Aufgaben nach aktuell geltendem Recht umzusetzen.

Diese Datenschutz-Checkliste kann nicht auf Einzelfälle eingehen und stellt keine Rechtsberatung dar, sondern ist lediglich eine Wissenssammlung, die aus umfangreicher Recherche, eigener Erfahrung und »best practices« verschiedener Entwickler zusammengetragen wurde und beständig weiter entwickelt wird. Wir übernehmen keine Haftung und empfehlen, in jedem Fall für rechtliche Fragen einen Rechtsanwalt zu konsultieren.

1. Sicherheit

SSL/TLS-Transportverschlüsselung Webseite

Transportverschlüsselung sollte immer dann verwendet werden, wenn personenbezogene Daten übertragen werden, insbesondere bei sämtlichen Formulardaten. Viele Browser warnen bei unverschlüsselten Verbindungen - besser wäre also eine durchgängige Transportverschlüsselung, egal, ob Formulare used Werden oder Nicht.

- ☐ Besteht auf jeder Unterseite eine HTTPS-Verschlüsselung?
- ☐ Weisen alle internen Links auf eine HTTPS-Adresse oder besteht existiert Mixed-Content?
- ☐ Sind externe Links erreichbar? Dies sollte überprüf werden, da zur Zeit viele Seiten auf HTTPS umgestellt werden (alte Links könnten nicht funktionieren)
- ☐ **Optional:** Es kann HSTS (»HTTP Strict Transport Security«) eingesetzt werden, um Angreifern die Möglichkeit zum »HTTP Downgrading« zu nehmen.

Sofern es der Webhoster (mit automatischer Verlängerung) zulässt, auf »Let's Encrypt«-Zertifikate setzen (kostenlos).
Für die (regelmäßige) Überprüfung externer Links (Broken Link Checker) kein WP-Plugin verwenden, weil es die Performance stark belastet.
Weiterleitungen von HTTP auf HTTPS wahlweise per »Force SSL«-Funktion des Hosters (wenn angeboten) oder per .htaccess konfigurieren.

Sicherheitskonzept des CMS (zB WordPress)

- ☐ Für den Schutz vor Brute-Force- und Wörterbuch-Attacken reicht ein Schutz, der die Anzahl der falschen Eingaben begrenzt.
- ☐ Für den Schutz vor Kommentar-SPAM reicht ein Schutz, vorzugsweise per Honeypot-Methode (reCaptcha nicht DSGVO-konform!).
- ☐ Für den Schutz vor Sicherheitslücken CMS-Installation, Plugins, Module und Themes (auch nicht aktivierte) immer aktuell halten!
- ☐ Für den Schutz vor Sicherheitslücken so wenig Plugins/ Themes wie nur möglich zu installieren!

Zugriffsprotokolle

- ☐ In den Zugriffsprotokollen des Servers gespeicherte personenbezogene Daten (insbes. die IP-Adresse) sollten nach Möglichkeit pseudonymisiert werden.
- ☐ Alternativ kann im Zuge der Datensparsamkeit komplett auf die Speicherung der IP-Adresse (sofern vom Webhoster zugelassen) verzichtet werden.
- ☐ Auch die Speicherdauer sollte wenn möglich auf 7 - 14 Tage verkürzt werden.

Webseiten-Installation

- ☐ Alle auf dem Server personenbezogenen Daten gelten auch als »Verarbeitung« - Auftragsverarbeitungsvertrag (AVV) mit Webhoster abschließen!

2. Externe Dienste

Analyse-Tools (z.B. Google Analytics, Matomo/ Piwik, WordPress Stats/ Jetpack)

Wichtig: Analyse-Tools, die personenbezogene Daten in den USA speichern, sind seit 2020 nach dem Schrems-II-Urteil nicht DSGVO-konform! Darunter gefallen u.a. Google Analytics und Jetpack .

- ☐ Abwägen, welches Analysetool unter der Berücksichtigung des Daten-sparsamkeits-Prinzips geeignet erscheint.
- ☐ Abwägen, ob ein Verarbeitungsgrund nach Art. 6 Abs. 1 lit. b) - f) DSGVO vorliegt oder nach Art. 6 Abs. 1 lit. a) Ein vorheriges Einverständnis eingeholt werden sollte.
- ☐ Sofern Cookies gespeichert werden, über einen Cookie-Banner darüber informieren und die Opt-Out-Funktion bereit stellen.
- ☐ Altdaten, die die maximale Verarbeitungszeit überschreiten, müssen händisch gelöscht werden.
- ☐ Google Analytics : AVV abschließen, minimale Verarbeitungszeit (14 Monate) einstellen, Targeting-Funktionen ausstellen, IP-Adressen pseudonymisieren.
- ☐ Matomo/ Piwik : AVV mit Webhoster abschließen, IP-Adressen pseudonymisieren, Speicherdauer einstellen.
- ☐ Webalizer : AVV mit Webhoster abschließen, IP-Adressen in den Server-Logs pseudonymisieren
- ☐ WP Stats / Jetpack : Da es derzeit keinen AVV für Jetpack gibt, das Plugin vollständig abschalten!

Wenn Sie die Auswertungmöglichkeiten von Google Analytics benötigen, sprechen Sie uns gern an. Wir zeigen Ihnen Datenschutzkonforme Alternativen.
Für eine einfach Nutzer-Statistik gibt es ebenfalls WordPress-Plugins die Sie mit wenigen Einstellungen nutzen dürfen.

Marketing-Tools (zB Google Ads, Affiliate-Netzwerke)

Wichtig: Marketing-Tools, die personenbezogene Daten in den USA speichern, sind seit 2020 nach dem Schrems-II-Urteil nicht DSGVO-konform! Darunter fallen ua Google Ads (insbes. die Remarketing-Funktion) und diverse Affiliate-Netzwerke.

- ☐ Google Ads verlangt derzeit das vorherige Einverständnis (Opt-In) lt. Programm-richtlinien , nicht nur für die Cookies und Beacons (Zählpixel), sondern auch für die Übertragung beliebiger personenbezogener Daten. Funktionen wie Remarketing oder die Auslieferung von personenbezogener Werbung sind derzeit fraglich und sollten - zumindest vorübergehend - abgeschaltet werden.
  Richtlinien bzw. AGBs bei sämtlichen Affiliate-Netzwerken beachten!
- ☐ Widgets, grafische Einbettungen oder JavaScript-Einbettungen von Werbemitteln von Affiliate-Netzwerken mindestens in der DSE erwähnen (sicherer: 2-Klick-Lösung)
- ☐ Werbemittel in beliebiger Form sollten als »Werbung« oder »Anzeige« gekennzeichnet werden!

Newsletter-Tools (zB Mailchimp, Clicktipp, Sendinblue, Jetpack Abonnement)

Wichtig : Newsletter-Tools, die personenbezogene Daten in den USA speichern, sind seit 2020 nach dem Schrems-II-Urteil nicht DSGVO-konform! Darunter gefallen u.a. Mailchimp und Jetpack .

- ☐ Newsletter-Formulare sollten mit einem angemessenen Hinweistext versehen und in der E-Mail beim Double-Opt-In-Verfahren wiederholt werden.
- ☐ Ein Newsletter-Eintrag sollte nicht an eine (kostenlosen oder kostenpflichtigen) Dienstleistung gekoppelt werden (»Kopplungsverbot«)
  Das Einverständnis für Newsletter-Einträge muss dokumentiert (Hinweistext, Zeitpunkt) und es muss ein Opt-Out bereit gestellt werden

Kopplungsverbot : Ein angebotenes Freebie darf nicht von der Zustimmung zur Erhebung personenbezogener Daten abhängig gemacht werden. »Als Dankeschön erhalten Sie [...]« wäre aber machbar. AVV mit dem Drittanbieter abschließen.

Möchten Sie Newsletter in Ihrem Unternehmen einsetzen und suchen nach einer Lösung die Datenschutzkonform ist, dann sprechen Sie uns gern an. Wir richten Ihnen ein Tool auf und sogenannte CTA (Call-To-Actions) - also Bereiche auf Ihrer Website ein, die das Eintragen für Ihre Website-Besucher attraktiver macht.

Social Plugins (z.B. Facebook, Instagram, Twitter)

Wichtig : Social Plugins, die personenbezogene Daten in den USA speichern, sind seit 2020 nach dem Schrems-II-Urteil nicht DSGVO-konform! Dies betrifft u.a. Facebook , Instagram und Twitter .

- ☐ Sämtliche eingebundene Social Plugins laden personenbezogene Daten bereits beim Besuch der Webseite. Sofern der User im sozialen Netzwerk eingeloggt ist, erfolgt eine genaue Zuordnung sowie eine Art »Bewegungsprofil« über alle mit Social Plugins versehenen Webseiten.
- ☐ Bei Login-Verfahren (zB Facebook Connect) und Kommentarfunktionen mit Verknüpfung zu sozialen Netzen wird ebenso verfahren.
- ☐ Sharing-Buttons, die die Anzahl der Shares anzeigen, haben das gleiche Problem.
- ☐ Einzelne reine Links (Text oder Grafik) sind DSGVO-konform.
- ☐ Beacons (Zählpixel) für Statistik-Zwecke sind ebenfalls sehr kritisch zu bewerten.

Vor dem Laden des Social Plugins über die Datenverarbeitung informieren (2-Klick-Lösung) oder Social Plugins komplett abschalten.
Facebook Connect, Jetpack Kommentarfunktion (und ähnliche) komplett abschalten.
Sharing-Buttons entweder ohne Kennzahlen anzeigen oder das WP-Plugin Shariff verwenden.

Webfonts (zB Google Fonts, Adobe Typekit, Fontawesome)

- ☐ Für den Einsatz von Webfonts ist immer eine Einwilligung erforderlich!
- ☐ Alternativ können Google Fonts, Adobe Typekit- und Fontaweome-Fonts (BootstrapCDN) lokalisiert werden (siehe CDNs)!
- ☐ Fonts könnten unter Umständen auch gegen andere lokale Open-Source-Fonts oder sogar dem CSS Font Stack ersetzt werden.

Google Fonts über den Google Webfonts Helper im (Child-)Theme lokalisieren.
Wenn nötig, CSS Fontstack einsetzen. Wer das WP-Plugin Autoptimize einsetzt, kann auch dort Google Fonts abschalten (funktioniert allerdings nicht immer).

Profil bzw. Profilbilder (zB Gravatar, About.me)

Wichtig : Profil, die personenbezogenen Daten (zB Bilder) in den USA speichern, sind seit 2020 nach dem Schrems-II-Urteil nicht DSGVO-konform! Dies betrifft ua Gravatar und About.me .

- ☐ Profil- und/oder Avatarbilder sollten nach Möglichkeit lokalisiert oder abgeschaltet werden, da sie mit Sicherheit personenbezogene Daten enthalten.
- ☐ Die in WordPress fest integrierte Gravatar-Funktion sollte nicht nur wegen den Bildern, sondern auch in den im Bild-Link als Hash abgelegten E-Mail-Adressen komplett abgeschaltet werden.

Emojis/ Emoticons (zB WP-Emojis)

- ☐ Wenn Emojis extern von einem CDN geladen werden, werden für gewöhnliche IP-Adressen beim Abruf abgerufen.
- ☐ Speziell bei den WP-Emojis wird zusätzlich Canvas Fingerprinting eingesetzt, was eine Zuordnung des Rechners ohne Speicherung von Cookies ermöglicht (auch, wenn keine Emojis angezeigt werden). Da diese Daten in den USA gespeichert werden, sind solche Emojis seit 2020 grundsätzlich nicht DSGVO-konform.
- ☐ WP-Emojis sollten daher immer abgeschaltet werden! Jeder moderne Browser zeigt trotzdem weiterhin Emojis und Emoticons an.

WP-Embeds/ oEmbeds

Wichtig : Die meisten oEmbeds speichern personenbezogene Daten in den USA und sind seit 2020 nach dem Schrems-II-Urteil nicht mehr DSGVO-konform!

- ☐ Wenn man bestimmte Links aus derzeit 34 Quellen (zB WordPress-Blogs, YouTube-Videos usw.) in den visuellen Editor in WordPress einfügt, werden sie automatisch in sogenannte oEmbeds umgewandelt. Dabei werden Teile der Zielwebseite per iframein die Webseite grafisch aufgearbeitet geladen. Beim Laden der Webseite werden damit automatisch alle Inhalte des iFrames mitgeladen (zB Analytics-Tools, Zählpixel).
- ☐ Sofern in den Posts, Seiten oder Kommentaren solche oEmbeds auftauchen, sollte die Funktion vollständig deaktiviert werden.
- ☐ Alte Einträge werden nicht vollständig entfernt und müssen händisch gelöscht werden.

oEinbettungen kann man vermeiden, insofern man Links in den Text-Editor von WordPress eingibt oder eigene Shortcodes verwendet.
Die gesamte Webseite (jede Unterseite) sollte auf iFrames getestet werden.
Bei positivem Ergebnis sollte die oEmbed-Funktion über die functions.php Child-Themes komplett entfernt werden. Alte Einträge müssen danach noch händisch gelöscht bzw. wieder zu normalen Links konvertiert werden.

Video- und Musikdienste (z.B. YouTube, Vimeo, Spotify, Soundcloud)

Wichtig: Video- und Musikdienste, die personenbezogene Daten in den USA speichern, sind seit 2020 nach dem Schrems-II-Urteil nicht DSGVO-konform!
Dies betrifft u.a. YouTube, Vimeo, Spotify und Soundcloud.

- ☐ Einbettungen von sämtlichen Video- und Musikdiensten übertragen bereits beim Laden der Webseite personenbezogene Daten und müssen deshalb über eine 2-Klick-Lösung verfügen. Zudem werden häufig auch Cookies gespeichert.
- ☐ YouTube-Videos können in einen »Erweiterten Datenschutzmodus« geschaltet werden, was aber nur die Speicherung von Cookies verhindert.

YouTube-Videos sollten nur im »Erweiterten Datenschutzmodus« erfolgen.
Einfachste Lösung: Video-Vorschauen manuell als Bild einbetten und auf die jeweiligen Plattformen verlinken 2-Klick-Lösung für alle Dienste kostenpflichtigen Cookie-Tool

Kartendienste (z.B. Google Maps, Open Street Maps, Mapbox, Leaflet)

Ebenso wie Video- und Musikdienste werden auch bei Kartendiensten bereits beim Laden der Webseite personenbezogene Daten erhoben und zumeist in den USA gespeichert.

☐ Auch hier bleibt derzeit nur eine 2-Klick-Lösung.

Einfachste Lösung: Kartenausschnitt manuell als Bild einbetten und auf die jeweilige Plattform verlinken.
Bei der Einbettung als Bild sollten Urheberrechts-Angaben direkt unter dem Bild angebracht werden. Screenshots von Google Mags können aus urheberrechtlichen Gründen nicht verwendet werden!
2-Klick-Lösung für alle Dienste kostenpflichtigen Cookie-Tool

Plugins/ Erweiterungen / Module

Plugins sollte genaustens überprüft werden, ob und wie personenbezogene Daten erhoben werden (für WordPress vgl. auch Blogmojo).

3. Impressum

☐ Das Impressum sollte von jeder Unterseite der Webseite aus über maximal 2 Klicks (z.B. »Kontakt« - »Impressum«) erreichbar sein.

☐ Das Impressum sollte alle Pflichtangaben gemäß §5 TMG enthalten, dazu gehören:
- Vor- und Zuname oder Firmenname und Geschäftsform sowie ggf. Inhaber
- Ladungsfähige Anschrift bzw. Adresse der Niederlassung
- Telefonnummer (oder Kontaktformular, wenn Reaktionszeit binnen 30 - 60 min.)
- E-Mail-Adresse
- USt-ID (oder Hinweis auf Befreiung) oder Wirtschafts-ID (keine Steuernummer!)
- Eintrag des Handelsregisters, Vereinsregisters, Genossenschaftsregisters oder Partnerschaftsregisters (wenn vorhanden)
- Behördliche Zulassung mit Angaben zur Aufsichtsbehörde, sofern der Beruf zulassungspflichtig ist
- Zuständige Kammer (Anschrift, Telefonnummer, Webseite) bei kammergebundenen Berufen (z.B. Rechtsanwälte, Steuerberater, Ärzte)
- Entsprechende Kennzeichnung, wenn sich die Gesellschaft in Abwicklung oder Liquidation befindet (nur AG, KGaA und GmbH)

☐ - Wenn das Stamm- oder Grundkapital (GmbH, freiwillig) angegeben wird, muss dies korrekt erfolgen.

Die Datenschutz-Checkliste

Open Source Checkliste um datenschutz-relevante Aufgaben nach aktuell geltendem Recht umzusetzen.

- ☐ Sofern auf der Webseite Dienstleistungen angeboten werden, gelten Informationspflichten gemäß 2 Abs. 1 DL-InfoV vor Vertragsschluss oder Erbringung der Leistungen. Diese können auch an zentraler Stelle ins Impressum geschrieben werden. Zusätzlich zu den obigen Angaben wären dann noch folgende Punkte notwendig:
  - Angaben zur Berufshaftpflichtversicherung (wenn vorhanden)
  - Geltende Allgemeine Geschäftsbedingungen (AGB)
  - Anwendbares Recht und Gerichtsstand
  - Bestehende Garantien (sofern vorhanden)

  Sollte die Webseite journalistisch-redaktionelle Inhalte enthalten (z.B. bei einem Blog), muss auch nach 18 Abs. 2 MStV ein inhaltlich Veranwortlicher mit Name und Adresse angegeben werden (Achtung, siehe Anmerkungen!).
  Online-Händler, die Waren an Verbraucher verkaufen, müssen zwingend einen Link zur Streitschlichtungsstelle der EU setzen
- ☐ Das Impressum muss barrierefrei sein! Anschrift, Telefonnummer oder Mail-Adresse als Bild oder in kodierter Form sind nicht zulässig!
- ☐ Haftungsausschlüsse/ Disclaimer zu Links und Inhalt gehören nicht (in verallgemeinerter Form) ins Impressum!
- ☐ Wer es noch nicht verstanden hat: »Das LG Hamburg hat 1998 entschieden...« ist Blödsinn und kann sogar zu Abmahnungen führen!
- ☐ »Keine Abmahnung ohne vorherigen Kontakt« entfaltet keine Wirkung!
- ☐ Ein Hinweis auf das eigene Urheberrecht kann gemacht werden, ist aber in Deutschland nicht zwingend notwendig.
- ☐ Das Impressum ist auch ein schöner Ort, um auf Miturheber wie den Designer, Webentwickler, Font-Ersteller usw. hinzuweisen.
- ☐ Bildnachweise gehören nur dann ins Impressum, wenn sie allgemeingültig für die ganze Webseite sind! (»Sofern nicht anders angegeben...«)

Anmerkungen

Seit November 2020 hat der Medienstaatsvertrag (MStV) den Rundfunkstaatsvertrag (RStV) abgelöst. Dementsprechend ändern sich die Angaben zum inhaltlichen Verantwortlichen von 55 Abs. 2 RStV zu 18 Abs. 2 MStV. Nicht vergessen, diese Pflichtangaben bei journalistisch-redaktionellen Inhalten (z.B. bei einem Blog) umzustellen!
Des weiteren könnten in zukünftigen Rechtssprechungen Angaben zur (freiwilligen) Selbstkontrolle zwecks Qualitätssicherung sowie zur entsprechenden Beschwerdestelle (vgl. 19 MStV) notwendig werden.

Tipps zur Umsetzung

Sprechen Sie uns auf das Thema Impressum an, wir bieten Ihnen ein Erstellungs-Tool mit dem Sie die Erstellung vom Anwalt abgesegnet und mit Siegel auf Ihrer Website einfach und schnelle einbinden können. Dieses wird Sie auch regelmäßig auf neue Rechtsstände hinweisen und eine Anpassung empfehlen.

4. Datenschutzerklärung

- ☐ Die Datenschutzerklärung (DSE) sollte von jeder Unterseite aus in einem Klick (evtl. auch in 2 Klicks, vgl. Impressum) erreichbar sein.
- ☐ Die DSE sollte ausführlich, aber verständlich und durch Rechtsgrundlagen der DSGVO und des BDSG-neu belegt sein.
- ☐ Doppelte DSEs (einmal kurz & verständlich, einmal lang & ausführlich) werden i.d.R. anerkannt (nicht mehr als 2 Klicks!)
- ☐ Die DSE sollte einen Gültigkeitsbereich (z.B. auch andere benannte Webseiten und soziale Medien) sowie ein Aktualisierungdatum enthalten.
- ☐ Die DSE kann durch einen (kostenlosen oder kostenpflichtigen) Generator oder direkt durch einen Anwalt oder Datenschutzbeauftragten erstellt werden.
- ☐ Für Presseerzeugnisse/ journalistische Zwecke weichen die Vorgaben zur Datenverarbeitung sowie die Informationspflichten nach §23 Abs. 2 & 3 MStV (des Bundeslandes) im Einklang mit Art. 85 DSGVO ab (»Medienprivileg«).

Anmerkungen
Seit dem Inkrafttreten des Medienstaatsvertrags (MStV) im November 2020 haben sich die datenschutzrechtlichen Vorgaben zum »Medienprivileg« bei journalistisch redaktionellen Inhalten geändert, siehe §23 MStV.

Tipps zur Umsetzung
Sprechen Sie uns auf das Thema Datenschutzerklärung an, wir bieten Ihnen ein Erstellungs-Tool mit dem Sie die Erstellung vom Anwalt abgesegnet und mit Siegel auf Ihrer Website einfach und schnelle einbinden können. Dieses wird Sie auch regelmäßig auf neue Rechtsstände hinweisen und eine Anpassung empfehlen.

Hinweis zum Thema Datenschutz
All unsere Website-Projekte beinhalten ein komplettes Datenschutzpaket, das alle Vorgaben der DSVO einhält. Wir können Ihnen aber auch individuelle Angebote für bestehende Websites anbieten.