fix&fertig.
Datenschutzhilfen
für Zivilgesellschaft

Checkliste
Datenschutz auf der Webseite

Was sind Cookies?

Der Begriff Cookie stammt aus dem Englischen und bedeutet wörtlich übersetzt „Keks". In der IT handelt es sich bei einem Cookie um eine Textinformation, die von einer besuchten Website über den Browser auf dem Rechner der Besucher:in gespeichert wird. Einige Cookies sind notwendig, um bspw. eine Webseite technisch korrekt anzuzeigen, andere werden genutzt um bspw. Nutzverhalten zu dokumentieren. [1]

Was ist ein (guter) Cookie-Banner?

Ein Cookie-Banner ist ein, einer Webseite vorgeschaltetes, Element, mit dem Besucher:innen wählen können, welche Cookies Sie auf dieser Webseite erlauben möchten.[2] Seit Einführung der DSGVO muss möglich sein, über einen Cookie-Banner die Aktivierung von Cookies zu steuern, die über die technisch notwendigen Cookies zur korrekten Auslieferung der Webseite hinausgehen. Diese Zustimmung muss aktiv passieren (ein vorgesetzter Haken darf nur bei „nur technisch notwendige Cookies" stehen) und zumindest mit einem Link versehen sein zu den Datenschutzinformationen. Manche Cookie-Banner erlauben sehr detaillierte Steuerungen – oft wird lediglich zwischen „technisch notwendigen" und „für Analyse- und Werbezwecke" unterschieden. Eigentlich sollten beide Möglichkeiten optisch gleichgestellt angeboten werden – dagegen wird sehr häufig verstoßen.

Eine gute Einführung in das Thema Vereinswebseite mitsamt der Erklärung der wichtigsten Begriffe wird auch von der Stiftung Datenschutz angeboten:
https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/webseiten-271

Webseite geprüft?

- ☐ Alle Fotos auf der Webseite dürfen auch dort veröffentlicht werden.
  - Dürft Ihr Fotos im berechtigten Interesse veröffentlichen oder besteht, wo nötig, eine zweckspezifische Einwilligung durch die abgebildeten Personen?[3]
- ☐ Videos sind korrekt eingebettet.[4]
- ☐ Es besteht ein Überblick über alle Cookies, die tatsächlich auf der Webseite laufen.
  - Kostenlose Cookie-Check-Angebote[5] prüfen meist nur die Seite, die als Adresse eingegeben wurde. Unterseiten (bspw. Spendenseite) werden dabei nicht automatisch miterfasst. Also ggf. wichtigste Seiten einzeln prüfen.

[1] Bei CHIP kann man sich näher zur Unterscheidung von – etwas polemisch ausgedrückt – „guten" und „bösen" Cookies informieren: https://praxistipps.chip.de/was-sind-cookies-eine-kurzerklaerung_9760
[2] https://www.ccm19.de/cookie-banner.html
[3] Siehe Praxisratgeber der Stiftung Datenschutz: https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/fotos-und-datenschutz-275 oder den Überblick zu Fotos im Vereinsleben der bayrischen Aufsichtsbehörde: https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Bilder_und_Verein.pdf
[4] Zur Einbindung von Videos in eigene Webseiten gibt es eine Handreichung der baden-württembergischen Datenschutzbehörde: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/11/20221107_Einbindung-Videos.pdf
[5] Eine Übersicht verschiedener Cookie-Checker gibt es von der Digitalagentur Verdure: https://www.verdure.de/magazin/technologie/cookie-checker-tools-website/

☐ Unnötige Cookies wurden entfernt. Die Zwecke für die übrigen Cookies sind klar.

- Facebook, Twitter, Instagram bieten „praktische" PlugIns an: Beim Click auf das Symbol landen Besucher:innen direkt auf der entsprechenden Social Media Seite – gleichzeitig werden von den Social Media Unternehmen jede Menge Daten über das Nutzverhalten der Besucher:innen verarbeitet und für gewerbliche Zwecke ausgewertet. Der Service einer ansprechenden Verlinkung lässt sich aber auch deutlich sparsamer erreichen durch die Platzierung einer einfachen Bilddatei des jeweiligen Logos (wird von allen Social Media Diensten angeboten[6]) mit einer Verlinkung zur jeweiligen Seite.
- Wenn bisher keinerlei Auswertung der Webseiten-Nutzung stattfindet, dann kann man sich und Besucher:innen auch die Analyse-Daten sparen und bspw. Google-Analytics schlicht deaktivieren.
- Werden externe Online-Dienste mit dazugehörigen Formularen (bspw. Fundraising, Newsletter) genutzt, dann sollte darunter immer ein kurzer Hinweis auf den externen Dienst platziert werden mit einer Verlinkung auf die Datenschutzinformationen auf der Webseite
- Wenn nur technisch notwendige Cookies laufen, dann braucht es auch keinen Cookie-Banner.

☐ Schriften sind datenschutzkonform in die Webseite eingebunden.

- Aktuell rollt eine Abmahnungswelle durch DTL wegen unerlaubter Einbettung von Google-Schriften, die jedes Mal extern über den US-amerikanischen Google-Server geladen werden. GoogleFonts lassen sich aber auch lokal hosten – dann ist alles fein.
- Der Art der Einbettung von GoogleFonts lässt sich gut über die Seite https://sicher3.de/google-fonts-checker/ prüfen. Auch hier wird immer nur die jeweilige Zielseite geprüft, aber aller Wahrscheinlichkeit werden die Schriften auf allen Unterseiten auf die gleiche Weise geladen wie auf der Startseite.
- Wenn nicht Euer Webseiten-Host helfen kann, dann gibt es unter eRecht24 eine Anleitung zur DSGVO-konformen Einbettung von GoogleFonts[7] sowie europäische Alternativen[8].

☐ Alle Formulare sind korrekt.

- Wenn Ihr Formulare anbietet (bspw. Kontaktformular, Spendenformular, Newsletter-Abo), dann unbedingt darauf achten, dass nur die jeweils erforderlichen Informationen als Pflichtfelder abgefragt werden (bspw. Newsletter – E-Mail, sonst nichts).
- Formulare dürfen nur dann „abgeschickt" werden, wenn vorher der Datenverarbeitung aktiv zugestimmt wurde (durch Haken setzen) und ein Hinweis zur Datenverarbeitung inkl. Zweckbeschreibung (Newsletter-Anmeldung, Veranstaltungsanmeldung, Spendenverwaltung) besteht mit Link zur Datenschutzinformation der Webseite. Bei einem einfachen Kontaktformular braucht es diese Zustimmung nicht – aber ein Hinweis auf die Datenverarbeitung bei der Nutzung des Formulars macht auch hier Sinn in Form eines einfachen Links zur Datenschutzerklärung.
- Nutzt Ihr bei Formularen PlugIns von externen Diensten, dann sollten diese als solche erkennbar sein, oder im Satz zu den Datenschutzhinweisen nochmal genannt werden („Hinweise zur Datenverarbeitung bei der Nutzung des XY-Formulars findest Du in unserer Datenschutzerklärung (LINK)").
- Beim Newsletter sollte auch auf die Widerrufsmöglichkeit hingewiesen werden.
- Es gilt bei allen „Angeboten" ein Kopplungsverbot (bspw. Veranstaltungsanmeldung darf nicht zwingend mit NewsletterAnmeldung verknüpft werden).

[6] Bspw. https://www.facebook.com/brand/resources/facebookapp/logo/
[7] https://www.e-recht24.de/artikel/datenschutz/13052-datenschutz-und-google-fonts.html
[8] https://european-alternatives.eu/alternative-to/google-fonts

☐ Die Webseite ist ausreichend gut verschlüsselt.

- Sobald Ihr ein Formular nutzt, besteht die Pflicht zu einer erhöhten Verschlüsselung (HTTPS-Pflicht).[9] Am besten über den Webseiten-Host einrichten lassen.

☐ Wo nötig sind Auftragsverarbeitungsverträge (AVs) mit externen Datenverarbeiter-Diensten abgeschlossen worden.

- Wenn externe Dienste in Eurem Auftrag Daten verarbeiten, dann muss das voraussetzbare Datenschutzniveau der Verarbeitung zugesichert werden ebenso wie der Ausschluss oder die Information über ggf. weitere Auftragsverarbeitung.
- Mittlerweile gibt es viele AVs auch automatisch digital bei Abschluss eines Accounts – aber in vielen Fällen ist es nach wie vor notwendig, bspw. mit dem Webseiten-Host einen AV abzuschließen.[10]
- Für Vereine sind AVs häufig ein überforderndes Thema. Im Zweifel einfach im Internet nach Auftragsverarbeitungsvertrag+Dienstleistung suchen – meist finden sich Hilfen dazu, wie man die konkreten AVs erhält bzw. abschließen kann.

☐ Datenschutzerklärung vollständig?

- Alle Cookies/PlugIns/externen Dienste müssen in der Datenschutzerklärung aufgeführt werden – ebenso wie nachgelagerte Datenverarbeitungsinformationen, wenn dabei eine Datenverarbeitung stattfindet, die von Personen nicht erwartet werden kann (bspw. wenn Ihr eine Kontaktverwaltungsdatenbank von einem US-amerikanischen Anbieter nutzt und alle Mitglieder, Spender:innen dort landen ODER wenn Ihr Daten weitergebt, ohne dass berechtigte Interessen hierfür die Grundlage bieten).
- Neben den zu erwartenden Datenverarbeitungen informiert die Datenschutzerklärung auch über die Rechte, die Personen haben, die auf Eure Webseite gehen (Betroffenenrechte), und nennt die Verantwortlichen (in der Regel geschäftsführender Vorstand / Verantwortliche:r im Sinne des Presserechts), die Beschwerdemöglichkeit bei der zuständigen Datenschutz-Aufsichtsbehörde und eine Kontaktmöglichkeit bei Fragen zum Thema Datenschutz.
- Es gibt eine Reihe von Text-Generatoren, die genutzt werden können – oft braucht es Ergänzungen. Achtet darauf, ob Ihr auch wirklich alle Datenverarbeitungen beim Generator eingeben konntet. Wenn nicht – einfach händisch ergänzen (aber nicht vergessen auf die Urheberschaft hinzuweisen).[11]

Stand: November 2022

[9] Gut erklärt von der Datenschutz Agentur: https://datenschutz-agentur.de/blog/wie-werden-webseiten-sicher-verschluesselt/
[10] Eine Erklärung und Übersicht der wichtigsten Verarbeitungsbereiche finden sich bei eRecht24: https://www.e-recht24.de/artikel/datenschutz/10580-auftragsdatenverarbeitung-adv-datenschutz.html
[11] Bspw. der WBS-Datenschutzgenerator: https://www.wbs.legal/it-und-internet-recht/datenschutzrecht/datenschutzerklaerung/datenschutzgenerator/ oder der Datenschutzgenerator der Stiftung Datenschutz: https://stiftungdatenschutz.org/ehrenamt/generator-datenschutzhinweise