Checkliste für Cookies und Web-Analyse im Webshop

Hinsichtlich DSGVO und TKG

Zur Verwendung dieser Checkliste:

In dieser Checkliste werden überblicksweise jene Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Telekommunikationsgesetzes (TKG) dargestellt, die beim Einsatz von Cookies und Webanalyse-Tools am Beispiel eines Webshops berücksichtigt werden müssen. Die einzelnen Punkte sind jeweils mit weiterführenden Informationen auf wko.at verlinkt.

Best-Practice-Beispiel für die allenfalls notwendige Einwilligung zu Cookies: „Abmahnung wegen nicht korrektem Einsatz von Tracking-Cookies – Auswirkungen der EuGH-Judikatur auf die Einbindung von Cookies".

1. **Setzen Sie Cookies ein, die personenbezogene Daten (z.B. IP-Adresse) verarbeiten?**
   Werden personenbezogene Daten verarbeitet, ist die DSGVO zu berücksichtigen. IP-Adressen werden als personenbezogene Daten qualifiziert.

   Für Cookies sind darüber hinaus die datenschutzrechtlichen Bestimmungen des TKG zu berücksichtigen. Nach dem TKG kommt es nicht darauf an, ob über Cookies personenbezogene Daten verarbeitet werden.

2. **Auf Basis welcher Rechtsgrundlage werden die Daten in Cookies verarbeitet?**
   Jede Datenverarbeitung benötigt eine der in der DSGVO genannten Rechtsgrundlagen (für Websites wichtigste Rechtsgrundlagen: Punkte a-d). Diese sind im Rahmen der Informationspflichten offen zu legen.

   a. **Liegt ein berechtigtes Interesse an der Datenverarbeitung vor?**

      Beispiele für ein berechtigtes Interesse:

      Datenverarbeitungen, die unbedingt erforderlich sind, damit der Webshopbetreiber (=Dienst der Informationsgesellschaft) seinen Dienst (z.B. Webshop), der vom Nutzer ausdrücklich gewünscht wird, anbieten kann, können nach § 96 Abs 3 TKG als berechtigtes Interesse gelten.

      Beispiel: Speicherung von IP-Adressen im Rahmen von Cookies für den Warenkorb.

      Im Rahmen der Informationspflichten (Datenschutzerklärung) ist das berechtigte Interesse anzuführen.

   b. **Ist die Datenverarbeitung zur Vertragserfüllung notwendig?**

   c. **Liegt eine gesetzliche Verpflichtung zur Datenverarbeitung vor?**

      (Bsp: steuerrechtliche Pflichten inkl. steuerrechtlicher Aufbewahrungsfristen)

   d. Im Fall einer über die notwendige Vertragserfüllung (bzw die Punkte a, b und c) hinausgehende Datenverarbeitung (**ACHTUNG**: für Cookies ist immer eine Einwilligung erforderlich, wenn es sich nicht um technisch notwendige Cookies handelt):

      i. **Ist die Datenverarbeitung mit dem ursprünglichen Verarbeitungszweck kompatibel?** oder:

      ii. **Liegt eine gültige Einwilligung des Nutzers vor?**

         i. Form der Einwilligung („opt in"; kein „opt out")?

         ii. Koppelungsverbot beachtet?

iii. Alterskontrolle bei Einwilligung von Kindern?

iv. Bei sensiblen Daten: ausdrückliche Einwilligung?

3. **Vor Vertragsabschluss: Alterskontrolle**

   Auf Einwilligungen gestützte Datenverarbeitungen von Kindern unter 14 Jahre sind nicht zulässig; Alterskontrolle sollte auch aus vertragsrechtlichen Gründen vor Vertragsabschluss erfolgen, da ansonsten unter Umständen kein gültiger Vertrag geschlossen werden kann und damit auch der Rechtsgrund der Vertragserfüllung problematisch werden könnte.

4. **Wie wird die Einhaltung der datenschutzrechtlichen Grundsätze gewährleistet?**

   Die in der DSGVO aufgezählten Grundsätze sind bei jeder Datenverarbeitung einzuhalten.

   a. Zweckbindung: **Für welche Zwecke werden die Daten in Cookies verarbeitet?**

      i. Zur Durchführung eines Einkaufs im Webshop?

      ii. Zur Webanalyse?

      Für jede Datenverarbeitung bedarf es eines konkreten legitimen Zwecks. Dieser ist im Rahmen der Informationspflichten (Datenschutzerklärung) offen zu legen. Die Verarbeitung für weitere Zwecke („Zweckverkettung") ist nur ausnahmsweise erlaubt (wenn der weitere Verarbeitungszweck mit dem ursprünglichen vereinbar ("kompatibel") ist.).

   b. **Ist sichergestellt, dass die Daten nur für die festgelegten, legitimen Zwecke und nicht zweckentfremdet verarbeitet werden?** (Bsp.: organisatorische Maßnahmen, klare Weisungen an Mitarbeiter sowie durch deren Schulung)

   c. **Datenminimierung**: Werden nur die für den jeweiligen Zweck notwendigen Daten erhoben?

   d. **Speicherbegrenzung:** Gibt es z.B. Löschkonzepte, Aufbewahrungsfristen?

   e. Welche **Datensicherheitsmaßnahmen** werden getroffen? (Bsp: Verschlüsselung, Pseudonymisierung, privacy by design, privacy by default)

   f. **Rechenschaftspflicht:** Wie kann die Einhaltung der datenschutzrechtlichen Pflichten nachgewiesen werden? (Bsp: Dokumentation im Verarbeitungsverzeichnis)

   g. Wie werden die **Informationspflichten der DSGVO** erfüllt? (Bsp: im Rahmen der Datenschutzerklärung)

   h. Wie werden die zusätzlichen Informationspflichten nach dem TKG (inkl. Angabe der Rechtsgrundlagen gem § 96 Abs 3 TKG) erfüllt? (Bsp: im Rahmen der Datenschutzerklärung)

   i. Datenrichtigkeit: Wie wird die sachliche Richtigkeit der Daten sichergestellt? (Bsp: Anweisung an Mitarbeiter, sachlich als unrichtig erkannte Daten zeitnahe zu berichtigen).

5. **Werden Auftragsverarbeiter eingesetzt?**

   Werden Auftragsverarbeiter eingesetzt, muss ein Auftragsverarbeiter-Vertrag geschlossen werden. Darüber hinaus ist in den Informationspflichten auf die Auftragsverarbeiter oder zumindest auf die Kategorie von Auftragsverarbeitern hinzuweisen.

   Beispiele für Auftragsverarbeiter: Webanalyse-Anbieter

6. **Besteht im Zusammenhang mit dem Betrieb des Webshops ein internationaler Datenverkehr?**

   Daten dürfen nur dann ohne Einwilligung in Drittstaaten (dh außerhalb der EU) übermittelt werden, wenn dort ein gleiches Schutzniveau herrscht (z.B. durch Standardvertragsklauseln/Angemessenheitsbeschluss der Europäischen Kommission. Dies ist im Rahmen der Informationspflichten (Datenschutzerklärung) offen zu legen.

7. **Wie werden die Betroffenenrechte gewährleistet?**

   Die Betroffenenrechte sind Teil der Informationspflichten (Datenschutzerklärung). Außerdem müssen organisatorische Maßnahmen getroffen werden, um ihnen im Fall ihrer Geltendmachung durch einen betroffenen Nutzer fristgerecht nachkommen zu können.

8. **Wie ist organisatorisch Vorsorge getroffen worden, dass im Falle einer Datenverletzung (z.B. Hackerangriff) den Meldeverpflichtungen gegenüber der Datenschutzbehörde und den Betroffenen fristgerecht nachgekommen werden kann?**

   Bei Datenverletzungen („data breach") bestehen Verständigungspflichten gegenüber der Datenschutzbehörde und den betroffenen Nutzern.

9. **Ist eine Datenschutz-Folgenabschätzung erforderlich?**

Wenn z.B. ein Webshop Kundenprofile („profiling“) erstellt, Webanalyse-Tools zur Auswertung des Nutzerverhaltens verwendet und/oder seine Kunden im Hinblick auf Kreditwürdigkeit überprüft, wird eine Datenschutz-Folgenabschätzung erforderlich sein.

10. **Sind die Datenanwendungen im Verarbeitungsverzeichnis dokumentiert?**

    Auch Datenanwendungen im Rahmen von Webauftritten müssen im Verarbeitungsverzeichnis dokumentiert werden.

11. **Ist ein Datenschutzbeauftragter zu bestellen?**

    Ein Datenschutz-Beauftragter wäre z.B. zu bestellen, wenn „profiling“ die Kerntätigkeit des Website-Betreibers darstellt. Dies wird bei Webshops idR nicht der Fall sein.

Stand: 18.01.2021