Datenverarbeitung im Webshop und auf der Website

Einwilligungserklärung - Cookies - Datenschutzerklärung

Allgemeines

Die Datenschutz-Grundverordnung (DSGVO) enthält neben anderen Bestimmungen auch detaillierte Informationspflichten sowie neue Spielregeln für allenfalls erforderliche Zustimmungserklärungen (Einwilligungserklärungen) für die Datenverarbeitung.

Für Anbieter von Diensten der Informationsgesellschaft (z.B. Betreiber von Webshops) gelten zusätzlich die Bestimmungen des Telekommunikationsgesetzes (§ 165 TKG). Diese Bestimmungen stammen nicht aus der DSGVO, sondern aus der E-Privacy-Richtlinie, die derzeit auf EU-Ebene überarbeitet wird und in eine eigene "E-Datenschutzverordnung" (E-DSVO) münden soll. Da derzeit noch nicht absehbar ist, wie die Änderungen im Detail aussehen werden und wann sie in Kraft treten werden, werden hier noch die derzeit geltenden Bestimmungen des TKG dargestellt.

Tipp:
Weiterführende Informationen zur DSGVO: wko.at/datenschutz

Tipp:
Verwenden Sie die "Checkliste für Cookies und Webanalyse im Webshop".

Achtung:
Beachten Sie bei einer Datenübermittlung in die USA den Entfall des Privacy-Shield-Abkommens!

Verarbeitung personenbezogener Daten

In jedem Webshop werden personenbezogene Daten verarbeitet; dies auch dann, wenn "bloß" Cookies gesetzt werden. Auch eine IP-Adresse (egal ob statisch oder dynamisch) wird als personenbezogenes Datum gesehen. In diesen Fällen sind die Bestimmungen der DSGVO sowie die diesbezüglichen datenschutzrechtlichen Bestimmungen des TKG einzuhalten.

1. Die Bestimmungen der DSGVO

Bei der Verarbeitung von Daten, wie etwa die Speicherung von Kundendaten, hat der dafür „Verantwortliche" (z.B. der Betreiber eines Webshops) im ersten Schritt die allgemeinen Grundsätze für Datenverarbeitungen einzuhalten. In einem zweiten Schritt hat er zu prüfen, auf welcher Rechtsgrundlage er eine Datenverarbeitung rechtmäßig durchführen kann. Zusätzlich ist stets darauf zu achten, dass die Informationspflichten erfüllt werden („Datenschutzerklärung"). Dies wird im dritten Schritt erläutert.

1.1 Die allgemeinen Grundsätze der DSGVO (Schritt 1)

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise (siehe dazu weiter unten), nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst sind. Der Grundsatz betrifft insbesondere die Informationen über die

Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie die Auskunft darüber, welche betreffenden personenbezogenen Daten verarbeitet werden.

Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Als nicht unvereinbar gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Zwecke oder für statistische Zwecke.

Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherzustellen haben, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden.

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

> **Achtung:**
> Der Datenverarbeiter (Website-Betreiber, „Verantwortlicher") ist für die Einhaltung der genannten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können („Rechenschaftspflicht").

1.2 Rechtmäßigkeit der Datenverarbeitung: Die Einwilligung und andere Rechtsgrundlagen (Schritt 2)

Rechtmäßig ist eine Datenverarbeitung dann, wenn sie neben der Einhaltung der oben beschriebenen Grundsätze auch auf Basis einer Rechtsgrundlage erfolgt.

Die **Einwilligung** durch den Betroffenen (des Nutzers der Webseite bzw des Kunden) ist eine Rechtsgrundlage.

Es gibt aber darüber hinaus auch weitere Rechtsgrundlagen, wobei zwischen „nicht sensiblen Daten" und „sensiblen Daten" zu unterscheiden ist:

1.2.1 Weitere Rechtsgrundlagen bei „nicht sensiblen Daten"

Bei „**nicht sensiblen Daten**" kann diese andere Rechtsgrundlage eine der folgenden Punkte sein.

Im Webshop typischerweise zur Anwendung kommende Rechtsgrundlagen:

- Die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist (z.B. Kaufvertrag im Webshop), oder zur Durchführung vorvertraglicher Maßnahmen (z.B. Befüllen des virtuellen Einkaufswagens vor dem Vertragsabschluss) erforderlich (soweit die vorvertraglichen Maßnahmen auf Anfrage der betroffenen Personen erfolgen).
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (z.B. arbeitsrechtliche oder steuerrechtliche Verpflichtungen).
- Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Letzteres ist insbesondere bei Kindern anzunehmen).

Hinweis:
Nach Erwägungsgrund 47 der DSGVO kann die Datenverarbeitung zum Zweck der Direktwerbung ein berechtigtes Interesse darstellen, wobei jeweils auf den Einzelfall abgestellt wird und das berechtigte Interesse daher stets im individuellen Fall geprüft wird. Ein berechtigtes Interesse ist aber stets dann anzunehmen, wenn das Cookie-Setzen aus technisch-funktionellen Gründen notwendig ist.

Im Webshop voraussichtlich seltener zur Anwendung kommende Rechtsgrundlagen:

- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Weiterverarbeitung für andere Zwecke:

Eine Datenverarbeitung zu anderen Zwecken als zu denjenigen, für den sie ursprünglich (rechtmäßig) verarbeitet wurden (Bsp: Kundendaten, die für eine Vertragsabwicklung erhoben wurden, sollen für Marketingzwecke verwendet werden), ist unter folgenden Voraussetzungen zulässig:

- Ohne Rücksicht auf die Vereinbarkeit der Zwecke der Verarbeitung ist eine Weiterverarbeitung ausschließlich zulässig, wenn:
    - eine Einwilligung dafür vorliegt, oder
    - eine gesetzliche Grundlage die Weiterverarbeitung vorsieht.
- In allen sonstigen Fällen muss die Weiterverarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben worden sind, vereinbar sein. Um diese Vereinbarkeit festzustellen ist Folgendes zu berücksichtigen:
    - jede Verbindung zwischen den ursprünglichen und neu beabsichtigten Zwecken
    - der Zusammenhang, in dem die Daten erhoben wurden
    - die Art der Daten (insbesondere ob sensible oder strafrechtlich relevante Daten vorliegen)
    - mögliche Folgen der Weiterverarbeitung für betroffene Personen
    - das Vorhandensein angemessener Garantien (z.B. Pseudonymisierung)

Liegt eine solche Vereinbarkeit mit den ursprünglichen Zwecken vor, ist keine andere gesonderte Rechtsgrundlage erforderlich, als diejenige für die (ursprüngliche) Erhebung der personenbezogenen Daten.

Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt als vereinbarter und rechtmäßiger Verarbeitungsvorgang.

Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, so muss er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung stellen.

Tipp:
Aus Rechtssicherheitsgründen ist bei einer Weiterverarbeitung zu anderen Zwecken als zu den ursprünglich empfohlenen, auch zu prüfen, ob eine andere Rechtsgrundlage (z.B. eine gesetzliche Verpflichtung) vorliegt bzw herbeigeführt werden kann (z.B. eine Einwilligungserklärung).

Achtung:
Auf jeden Fall muss der Nutzer nicht nur über den ursprünglichen Verarbeitungszweck, sondern auch über die anderen Zwecke informiert werden, z.B. in der Datenschutzerklärung.

1.2.2 Weitere Rechtsgrundlagen bei „sensiblen Daten“

Bei „sensiblen Daten“ (personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben/sexuelle Orientierung) kann diese andere Rechtsgrundlage folgende sein:

- Die Verarbeitung sensibler Daten ist aus Gründen des Arbeitsrechts oder des Sozialrechts erforderlich, damit der Verantwortliche oder die betroffene Person den arbeitsrechtlichen oder sozialrechtlichen Verpflichtungen nachkommen kann.
- Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außer Stande, ihre Einwilligung zu geben.

- Die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien (z.B. verbindliche interne Datenschutzvorschriften, Zertifizierungen) durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemaligen Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakt mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.
- Die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat (aus einem Größenschluss ist wohl anzunehmen, dass auch nicht-sensible Daten bei offensichtlicher Veröffentlichung durch die betroffene Person selbst ebenfalls rechtmäßig verarbeitet werden dürfen).
- Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich.
- Die Verarbeitung sensibler Daten ist auf Grundlage gesetzlicher Vorgaben aus Gründen eines erheblichen öffentlichen Interesses erforderlich.
- Die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage von Gesetzen oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erforderlich.
- Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden, grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage von europarechtlichen oder nationalen Gesetzen erforderlich.
- Die Verarbeitung ist auf gesetzlicher Grundlage für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich.

1.2.3 Weitere Rechtsgrundlagen bei strafrechtsrelevanten Daten

Die Verarbeitung von Daten (gerichtlich oder verwaltungs-)**strafrechtlicher Verurteilungen und Straftaten** unterliegt einer gesonderten Regelung. Die Verarbeitung solcher Daten ist nur unter folgenden Voraussetzungen zulässig:

- es besteht eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Datenverarbeitung oder
- die Datenverarbeitung ergibt sich aus gesetzlichen Sorgfaltspflichten oder zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. In diesen Fällen ist die Art und Weise der Verarbeitung so vorzunehmen, dass die Wahrung der Interessen der betroffenen Person gewährleistet wird.

1.2.4 Die Einwilligungserklärung

Sind keine der unter 1.2.1 bis 1.2.3 genannten Rechtsgrundlagen vorhanden, ist von der betroffenen Person eine Einwilligung einzuholen.

> **Tipp:**
> Prüfen Sie bevor Sie eine Einwilligung einholen zunächst, ob nicht bereits eine andere Rechtsgrundlage für die Datenverarbeitung vorliegt (in diesem Fall wäre keine Einwilligung notwendig).

Unter einer „Einwilligung" versteht die DSGVO jede **freiwillig**, für den **bestimmten Fall**, **in informierter Weise** und **unmissverständlich** abgegebene Willensbekundung durch die betroffene Person in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Daraus folgt, dass eine Einwilligungserklärung etwa schriftlich, elektronisch (z.B. durch aktives Anklicken einer vorformulierten Einwilligungserklärung), aber auch in konkludenter Form (schlüssig) erfolgen kann.

Ein bloßes Schweigen oder Untätigkeit der betroffenen Person kann keine Einwilligung darstellen, sofern nicht andere sonstige Begleitumstände eindeutig auf ein Zustimmen zur Datenverarbeitung hinweisen.

Achtung:
Vorformulierte Einwilligungserklärungen im Internet, die bereits ein zustimmendes Häkchen vorfinden, gelten nicht als gültige Einwilligungserklärung.

Achtung:
Bei der Verarbeitung sensibler Daten muss jedenfalls eine ausdrückliche Einwilligungserklärung (keine konkludente Einwilligung) vorliegen.

Tipp:
Aus Beweisgründen und aufgrund der Rechenschaftspflicht ist anzuraten, dass der Verantwortliche auch bei der Einwilligungserklärung von nicht-sensiblen Daten schriftliche Einwilligungserklärungen oder sonstige nachweisbare Einwilligungserklärungen einholt.

1.2.4.1 Wann ist eine Einwilligung „freiwillig"?

„Freiwillig" ist eine Einwilligungserklärung dann, wenn der Betroffene seine Einwilligung insbesondere ohne Zwang und nach freier Entscheidungsmöglichkeit abgegeben hat.

Freiwilligkeit ist insbesondere dann zweifelhaft:

- wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert Einwilligungserklärungen erteilt werden können, obwohl es im Einzelfall angebracht ist;

  Tipp: Holen Sie für jeden Verarbeitungszweck eine gesonderte Einwilligung ein.

  Beispiel:

  O Ja, ich stimme dem Erhalt eines wöchentlichen E-Mail Newsletters des Unternehmens XY, gesendet an folgende E-Mail-Adresse ..... zu.

  O Ja, ich stimme darüber hinaus dem Erhalt eines wöchentlichen E-Mail-Newsletters des Unternehmens AB, gesendet an die oben angeführte E-Mail-Adresse zu.

  Ich kann jede dieser Einwilligungen jederzeit, auch getrennt und auch bei jedem Erhalt des Newsletters, widerrufen. Durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Zustimmung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

- wenn die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung des Vertrages nicht erforderlich ist (Koppelungsverbot);

Positives Beispiel:

O Ja, ich möchte die Ware XYZ zum Preis von AB kaufen.

O Ja, ich stimme dem Erhalt eines wöchentlichen E-Mail Newsletters des Unternehmens XY, gesendet an folgende E-Mail-Adresse ..... zu.

Ich kann diese Einwilligung jederzeit und auch bei jedem Erhalt des Newsletters, widerrufen. Durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Zustimmung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

So nicht:

O Ja, ich möchte die Ware XYZ zum Preis von AB kaufen und stimme zu, den wöchentlichen E-Mail-Newsletter des Unternehmens XY an folgende E-Mail-Adresse ..... zugestellt zu erhalten und nehme zur Kenntnis, dass ich diese Einwilligung jederzeit, auch bei jedem Erhalt des Newsletters, widerrufen kann.

- wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht (z.B. wenn es sich bei dem Verantwortlichen um eine Behörde handelt).

Nach der Judikatur kann eine Einwilligung auch dann freiwillig sein, wenn als Alternative zur Datenerhebung ein (moderates) Entgelt zur Nutzung der Website angeboten wird. Ist die Nutzung der Website ohne Einwilligung jedoch unmöglich, so liegt nach der Judikatur keine Freiwilligkeit mehr vor (siehe dazu Punkt 2.3 bezüglich Cookies).

1.2.4.2 Was ist mit „bestimmten Fällen" gemeint?

Eine weitere Voraussetzung für eine gültige Einwilligungserklärung ist, dass sie sich auf „bestimmte Fälle" beziehen muss. Daraus folgt, dass die betroffene Person im Rahmen der Einwilligungserklärung in Kenntnis gesetzt werden muss, welche Datenarten für welche konkreten Zwecke verarbeitet werden sollen.

Beispiel:
Zum Versand des Newsletters verarbeiten wir folgende Daten: Name, Adresse, E-Mail-Adresse.

1.2.4.3 Was ist mit „in informierter Weise" gemeint?

Nach der Definition muss eine Einwilligung durch den Betroffenen auch in "informierter Weise" erfolgen. So hat die (vorformulierte) Einwilligungserklärung vor allem in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zu erfolgen. Ist die Einwilligungserklärung z.B. in AGB eingebettet, die noch andere Sachverhalte mitumfassen (z.B. Regelungen über die Gewährleistung oder Zahlungsbedingungen) so muss sich die Einwilligungserklärung von den anderen Sachverhalten klar „unterscheiden".

Die Einbettung in AGB kann entweder durch eine Separierung erfolgen oder durch eine optische Hervorhebung innerhalb der AGB (z.B. durch Fettdruck und dicke schwarze oder sonstige farbliche Umrahmung).

Achtung:
Dabei ist allerdings immer auch das Koppelungsverbot zu beachten. Einwilligungen im Rahmen von AGB sind daher nur dann zulässig, wenn z.B. beim Bestellvorgang einmal gesondert die datenschutzrechtliche Einwilligungserklärung (für die E-Mail-Werbung) bestätigt oder abgelehnt werden kann und dann mit einem eigenen Klick die Gültigkeit der AGB bestätigt wird.

Tipp:
Eine datenschutzrechtliche Einwilligungserklärung im Rahmen von AGB ist daher nicht zu empfehlen, sondern sollte von den AGB textlich getrennt erfolgen.

Das Kriterium „in informierter Weise" setzt weiters voraus, dass spätestens zum Zeitpunkt der Einwilligung alle verpflichtenden Informationen der DSGVO zur Verfügung gestellt werden (z.B. entweder im Einwilligungstext selbst oder durch einen Link auf eine Datenschutzerklärung, die diese Informationen enthält).

Wird gegen dieses Transparenzgebot verstoßen, sind jene als intransparent zu wertenden Teile einer datenschutzrechtlichen Einwilligungserklärung nicht verbindlich.

Die betroffene Person hat jederzeit das Recht, ihre abgegebene Einwilligungserklärung zu widerrufen. Auf diese Möglichkeit ist die betroffene Person vor Abgabe der Einwilligung hinzuweisen.

Beispielhafter Formulierungsvorschlag:

„Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich ... [die Datenarten genau aufzählen, z.B. „Name", „Adresse", etc.] zum Zweck der ... [genaue Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte des Unternehmens in Form von Broschüren, Foldern und Mails ..."] bei dem Unternehmen NN verarbeitet werden und die Daten ..... die Datenarten genau aufzählen, z.B. „Name", „Adresse" etc.] zum Zweck der .... (genaue Zweckangabe z.B. „zur zentralen Abwicklung des Kunde-Beschwerdemanagements") an .... (genaue Angabe des Übermittlungsempfängers z.B. Name bzw. Firma der Konzernmutter mit Anschrift) weitergegeben werden.

Diese Einwilligung kann jederzeit bei ..... [Angabe der entsprechenden Kontaktdaten] widerrufen werden. Durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Zustimmung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Achtung:
Soll auch eine Weitergabe von Daten in Drittstaaten erfolgen, sind zusätzlich die Erfordernisse des internationalen Datenverkehrs zu berücksichtigen.

1.2.5 Besonderheiten bei Einwilligungserklärungen von Kindern

Im Falle von Zustimmungserklärungen im Zusammenhang mit Angeboten von Diensten der Informationsgesellschaft (z.B. Webshop), die einem Kind direkt gemacht werden, ist eine Datenverarbeitung personenbezogener Daten von Kindern vor Vollendung des 14. Lebensjahres nur dann rechtmäßig, sofern die Einwillligung von Obsorgeberechtigten (vor allem Eltern) oder mit deren Zustimmung erteilt wurde.

Achtung:
Neben dieser datenschutzrechtlichen Regelung sind für den Vertragsabschluss auch die zivilrechtlichen Bestimmungen für die Geschäftsfähigkeit zu berücksichtigen.

Um sich in solchen Fällen zur vergewissern, dass die Einwilligung durch die Obsorgeberechtigten für das Kind erteilt wurde, hat der Verantwortliche unter Berücksichtigung der verfügbaren Technik „angemessene" Anstrengungen zu unternehmen. Was darunter zu verstehen ist, dazu schweigt die DSGVO. Eine Altersabfrage, gegebenenfalls mit einer Zustimmungserklärung des Obsorgeberechtigten, ist empfehlenswert.

1.2.6 Bestehende Einwilligungserklärungen

Datenverarbeitungen, die auf bereits bestehenden Einwilligungserklärungen nach der alten Rechtslage gemäß Datenschutzgesetz 2000 (DSG 2000) basieren, erfordern keine neuerliche Einwilligungserklärung, sofern die erteilten Einwilligungen den Bedingungen der neuen Rechtslage entsprechen.

Achtung:
Fehlt allerdings eines der beschriebenen Elemente (wenn z.B. das neue Koppelungsverbot der DSGVO nicht eingehalten wurde), muss die Einwilligung neu eingeholt werden.

1.3. Informationspflichten nach der DSGVO (Schritt 3: „Datenschutzerklärung")

Nach der DSGVO sind die Betroffenen über die beim Verantwortlichen stattfindenden Datenverarbeitungen zu informieren. Diesen Informationspflichten kann durch Veröffentlichung einer „Datenschutzerklärung" auf der Website des Verantwortlichen nachgekommen werden.

Zusätzlich zu den allgemeinen Informationspflichten nach der DSGVO bestehen auch spezielle Informationspflichten nach dem TKG, die vor allem bei der Setzung von „Cookies" zu beachten sind.

Tipp:

Nach verschiedenen anderen Gesetzen (z.B. nach dem E-Commerce-Gesetz oder dem Mediengesetz) sind bereits etliche Informationen auf der Website zu veröffentlichen (z.B. im Impressum). Auch wenn es natürlich möglich ist, im Impressum auch den Informationspflichten nach der DSGVO nachzukommen, empfiehlt sich aus Transparenzgründen eine separate, eigenständige Zurverfügungstellung der datenschutzrechtlichen Informationen als „Datenschutzerklärung".

2. Sonderbestimmungen für Cookies nach dem TKG

2.1 Informationspflichten

Cookies nennt man Informationen, die vom Informationsanbieter (z.B. einem Webshop-Betreiber) mit Hilfe des Browsers auf der Festplatte des PC des Kunden abgespeichert werden, um Daten mit dem Computer des Kunden zu verknüpfen. Diese Technik wird z.B. beim virtuellen Einkauf angewendet. Durch das Setzen von Cookies können aber auch Webanalysen und Benutzerprofile erstellt werden.

In Cookies können sowohl personenbezogene als auch nicht personenbezogene Daten gespeichert werden. Wenn mit den in den Cookies gespeicherten Informationen ein Personenbezug hergestellt werden kann, sind die datenschutzrechtlichen Pflichten zu beachten.

Achtung:
IP-Adressen werden als personenbezogene Daten gesehen, da mit ihrer Hilfe ein Betroffener identifiziert bzw zumindest identifizierbar ist.

Aufgrund der Judikatur des EuGH („Planet 49") zur E-Privacy-Richtlinie sind auch bei der Verarbeitung von nicht-personenbezogenen Daten im Rahmen von Cookies (z.B. sehr verkürzte IP-Nummern ohne Möglichkeit, Rückschlüsse auf Personen zu erlangen, bspw. anonymisierte IP-Nummern) Informationen über den Vorgang der Verarbeitung dieser nicht-personenbezogenen Daten zu geben. Darüber hinaus sind zusätzlich auch Einwilligungen einzuholen, sofern nicht eine Ausnahme dafür besteht (siehe im Detail unten 2.3).

Achtung:
In den weiteren Ausführungen wird aufgrund der in der Praxis überwiegenden Datenverwendung von nicht-sensiblen Daten lediglich auf diese repliziert. Zur Definition von sensiblen und nicht-sensiblen Daten siehe oben Punkt 1.2.2.

Hinweis:
Die gegenwärtigen Sonderbestimmungen für „Cookies" stammen aus der E-Privacy-Richtlinie und dem Telekommunikationsgesetz (TKG). Derzeit wird die E-Privacy-Richtlinie auf EU-Ebene überarbeitet. Auf die in Diskussion stehenden Änderungen wird in diesem Merkblatt noch nicht eingegangen, da gegenwärtig noch nicht absehbar ist, was tatsächlich im Detail geändert wird. Die weiteren Ausführungen beziehen sich daher auf die gegenwärtige Rechtslage nach dem TKG.

Das TKG sieht eigene Informationspflichten vor: es ist darüber zu informieren,

- welche personenbezogenen Daten ermittelt, verarbeitet oder an Dritte übermittelt werden,
- auf welcher Rechtsgrundlage (z.B. aufgrund eines Vertrages, eines speziellen Gesetzes),
- für welche Zwecke dies erfolgt und
- wie lange die Daten gespeichert werden.

Diese Informationspflichten decken sich großteils mit den allgemeinen Informationspflichten der DSGVO.

Achtung:

Wie bereits oben ausgeführt, ist aufgrund der EuGH-Judikatur über sämtliche Informationen, die mittels Cookies verarbeitet werden, unabhängig davon, ob diese personenbezogen sind oder nicht, aufzuklären. Auch wenn das TKG nur auf personenbezogene Daten abstellt, wird aufgrund der EuGH-Judikatur empfohlen, auch unabhängig von einem Personenbezug darüber zu informieren, welche Informationen verarbeitet werden.

2.2 Datenschutzerklärung

Im Falle einer gemeinsamen Zurverfügungstellung mit den allgemeinen Informationspflichten nach der DSGVO muss dafür gesorgt werden, dass die Informationen jederzeit „klar und leicht zugänglich" sind. Es empfiehlt sich deshalb keine Veröffentlichung bloß im Impressum, sondern im Rahmen einer eigenen Datenschutzrubrik (z.B. eines eigenen Buttons „Datenschutzerklärung" oder „Privacy Policy").

Achtung:
Die sogenannte Artikel 29-Gruppe (aktuelle Bezeichnung: Europäischer Datenschutzausschuss-EDSA, dem Vertreter der nationalen Datenschutzbehörden angehören) hat in einem „Arbeitspapier" zur Rechtslage nach der „E-Privacy-Richtlinie" die Rechtsmeinung veröffentlicht, dass der Informationspflicht an „prominenter" Stelle in klarer und verständlicher Form nachgekommen werden muss, z.B. auf der Startseite. Nach dieser Rechtsmeinung scheint das „bloße" Anführen insbesondere der Informationen nach dem TKG, im Impressum ohne Zusatzinfo auf der Startseite problematisch. Die Informationserklärung muss allenfalls auch Hinweise beinhalten, „wie der User alle oder einzelne Cookies akzeptieren kann und wie er in der Zukunft seine Präferenz ändern kann".

Tipp:
Weisen Sie den Nutzer darauf hin, dass er in seinen Browsereinstellungen den Einsatz von Cookies auch verhindern kann.

Beispiel: Ein Webshop-Betreiber setzt Cookies, damit der Käufer mit einem virtuellen Einkaufswagen online bestellen kann. Dabei wird die IP-Nummer des Anschlussinhabers verarbeitet. Darüber hinaus speichert der Händler zum Zwecke der Vertragsabwicklung den Namen, die Anschrift und Kreditkartennummer des Käufers sowie die beabsichtigten Einkäufe. Ein Datenschutzbeauftragter ist nicht bestellt.

Eine Information könnte folgendermaßen lauten:

Beispielsweiser Formulierungsvorschlag:
„Wir weisen darauf hin, dass zum Zweck des einfacheren Einkaufsvorganges und zur späteren Vertragsabwicklung vom Webshop-Betreiber im Rahmen von Cookies die IP-Daten des Anschlussinhabers gespeichert werden, ebenso wie Name, Anschrift und Kreditkartennummer des Käufers sowie die ausgewählten Waren und das Kaufdatum. Darüber hinaus werden zum Zweck der Vertragsabwicklung folgende Daten auch bei uns gespeichert: ..... .

Eine Datenübermittlung an Dritte erfolgt nicht, mit Ausnahme der Übermittlung der Kreditkartennummer an abwickelnde Bankinstitute/Zahlungsdienstleister zum Zweck der Abbuchung des Einkaufspreises. Nach Abbruch des Einkaufsvorganges werden die bei uns gespeicherten Daten gelöscht. Im Falle eines Vertragsabschlusses werden sämtliche Daten aus dem Vertragsverhältnis bis zum Ablauf der steuerrechtlichen Aufbewahrungsfrist (7 Jahre) gespeichert. Die Daten „Name", „Anschrift", „gekaufte Waren" und „Kaufdatum" werden darüber hinaus gehend bis zum Ablauf der Produkthaftung (10 Jahre) gespeichert. Die Datenverarbeitung erfolgt auf Basis der gesetzlichen Bestimmung des § 165 Abs 3 TKG 2021 sowie des Art 6 Abs 1 lit a (Einwilligung) und/oder b (notwendig zur Vertragserfüllung) der DSGVO."

Den allgemeinen Informationspflichten der DSGVO könnte wie folgt nachgekommen werden:

„Datenschutzrechtlich verantwortlich: [Unternehmen XY]. Wenn Sie Fragen haben, kontaktieren Sie uns unter: [E-Mail-Adresse einfügen]. Ihnen stehen bezüglich Ihrer bei uns gespeicherten Daten grundsätzlich das Recht auf Auskunft, Richtigstellung, Einschränkung, Widerruf und Widerspruch zu einer Datenverarbeitung sowie Löschung und Übertragbarkeit Ihrer Daten zu. Wenn Sie glauben, dass wir gegen datenschutzrechtliche Vorschriften verstoßen, können Sie sich bei uns [E-Mail-Adresse einfügen] oder bei einer Datenschutzbehörde beschweren."

Achtung:
Dieses Beispiel wurde nur zum besseren Verständnis gewählt. Jeder Verantwortliche (Datenverarbeiter bzw Webshopbetreiber) muss selbst überlegen, welche konkreten Daten er von einem Nutzer für welche rechtlich zulässigen Zwecke benötigt.

2.3 Einwilligungserklärungen (Sonderbestimmungen nach § 165 Abs 3 TKG 2021)

Grundsätzlich hat der Verantwortliche bei der Verarbeitung (z.B. Speicherung) von personenbezogenen Daten (z.B. IP-Nummern) im Rahmen von Cookies nach dem TKG vor deren Verarbeitung eine informierte Einwilligung („auf Grundlage von klaren und umfassenden Informationen") einzuholen (z.B. bei Webtracking). Diese hat den Anforderungen für gültige Einwilligungserklärungen wie unter 1.2.4 beschrieben zu entsprechen. So ist vor allem darauf hinzuweisen, dass der Betroffene ein „aktives Verhalten" setzen muss („Opt-in"-Lösung); vorangekreuzte Einwilligungserklärungen durch den Verantwortlichen (etwa in Kästchen) führen zur Unwirksamkeit der Einwilligungserklärung. Ebenso ist vor allem auf das „Koppelungsverbot" hinzuweisen. Im Detail siehe die Ausführungen unter 1.4.2. Besonders bei Einwilligungen zu „Cookies" ist nach den Erläuternden Bemerkungen zu § 165 TKG 2021 auch darauf zu achten, dass eine Information zur Funktionsdauer der Cookies und der Drittempfänger erfolgt.

Achtung:

Aufgrund der EuGH-Judikatur („Planet 49“) ist auch bei sämtlichen Verarbeitungen von Informationen im Rahmen von Cookies, und zwar unabhängig davon, ob damit personenbezogene Daten verarbeitet werden (z.B. auch bei gekürzten IP-Nummern, aus denen grundsätzlich keine Rückschlüsse auf Personen gezogen werden können), eine Einwilligungserklärung einzuholen. Auch wenn das TKG nur auf personenbezogene Daten abstellt, wird aufgrund der EuGH-Judikatur empfohlen, auch unabhängig von einem Personenbezug mit einer Einwilligung zu arbeiten.

Lediglich in jenen Fällen bedarf es keiner vorherigen Einwilligung des Betroffenen, in denen der Anbieter eines Informationsdienstes (etwa ein Webshop-Betreiber) einen vom Betroffenen ausdrücklich gewünschten Dienst nur unter der Bedingung zur Verfügung stellen kann, dass Daten verwendet werden müssen und dies auch unbedingt erforderlich ist (funktionale Notwendigkeit. Bei IP-Datenspeicherungen im Rahmen von Cookies zum Zwecke des virtuellen Einkaufs mit begrenzter Speicherdauer („Warenkorb“) könnte dies so gesehen werden. Hier ist lediglich der Informationspflicht nachzukommen.

Ebenso keine Einwilligungserklärung muss eingeholt werden, wenn ein „Cookie“ technisch notwendig ist, eine Nachrichtenübertragung über ein Kommunikationsnetz durchzuführen und dies der alleinige Zweck ist.

Achtung:

Wenn nicht bloß „funktionelle“ Cookies (also z.B. technisch notwendige Cookies oder solche aus Sicherheitsgründen) gesetzt werden, sondern z.B. Cookies zu Tracking- oder Marketingzwecken und dafür eine Einwilligung einzuholen ist, ist für die Erfüllung des Prinzips der Freiwilligkeit (siehe Punkt 1.2.4.1) zu berücksichtigen, dass der Nutzer für den Fall der Nicht-Zustimmung grundsätzlich nicht an der Weiternutzung der Website gehindert werden darf. Wahlmöglichkeiten wie bspw. als Alternative „Daten“ oder „Entgelt“ für das Weiternutzen der Website sind nach der Judikatur zulässig, sofern durch die Höhe des Entgelts keine prohibitive Wirkung insofern entsteht, als der Nutzer von der Nutzung der Website faktisch abgehalten wird.

2.4 Form der Einholung einer allenfalls erforderlichen Einwilligungserklärung bei Cookies

Auch aufgrund der Judikatur des EuGH ist im Falle der Notwendigkeit einer Einwilligungserklärung als Rechtmäßigkeitsgrundlage (also bspw. bei Webanalyse-Cookies) eine aktive Einwilligung einzuholen. Eine konkludente Einwilligung in Form einer Browser-Einstellung wird nicht ausreichen.

Nähere Informationen dazu: „Abmahnung wegen nicht korrektem Einsatz von Tracking-Cookies – Auswirkungen der EuGH-Judikatur auf die Einbindung von Cookies“

Unzulässig ist auf jeden Fall eine „Opt-out“-Lösung (Vorkonfigurationen wie etwa vorangekreuzte Kästchen durch den Verantwortlichen).

Hinweis:
Die Artikel 29-Gruppe (aktuelle Bezeichnung: EDSA) hat bereits zur Rechtslage nach der „E-Privacy-Richtlinie“ in einem „Arbeitspapier“ die Rechtsmeinung veröffentlicht, dass es eines „aktiven Verhaltens“ des Users bedarf, um von einer gültigen Einwilligung zur Cookie-Setzung ausgehen zu können. Die Artikel 29-Gruppe führt dafür beispielhaft das Anklicken einer „Infobox“ an, in der die Datenschutzerklärung abgebildet ist.

Tipp:
Die Einholung der Einwilligung kann gleichzeitig mit dem Anbieten der entsprechenden Informationen erfolgen, indem zu Beginn der Session eine „Infobox“ erscheint, die der Nutzer sodann anklicken kann.

Relevante Artikel der DSGVO: Art 4 Z 11, Art 7, Art 8

Relevante Erwägungsgründe: 32ff, 171

Relevante Bestimmungen des DSG (idF des Datenschutz-Anpassungsgesetzes 2018): § 4

Relevante Bestimmungen des TKG 2021: § 165 Abs 3

Stand: 28.01.2022