lawlikes
RECHT einfach und verständlich

Checkliste DSGVO kompakt

Die EU-DSGVO schafft es in diesem Jahr, wie keine andere Verordnung vorher für echte Verunsicherung zu sorgen.

Sicherlich geht es dir auch so, dass du das Gefühl hast, überhaupt nicht durchzublicken. Sei ganz beruhigt, denn so geht es wirklich den Allermeisten gerade.

Es gibt online einfach viel zu viele Informationen und juristische Fachbücher zu dem Thema möchte ja auch keiner so gerne lesen… Dazu kommen Menschen, die Halbwahrheiten und Angst verbreiten - wie soll man da noch durchblicken?

Und sind wir mal ehrlich: Gesetze, Recht und Verordnungen - da ist einem doch der Zahnarztbesuch fast lieber 😉.

Drumherum zu reden hilft aber auch nicht, denn ab dem 25. Mai 2018 wird es aber soweit sein und die EU-Datenschutzgrundverordnung (DSGVO) tritt dann endgültig in Kraft und wird ab diesem Datum unmittelbar anwendbares Recht in allen EU-Staaten sein.

Also erstmal: DURCHATMEN und Kräfte sammeln!

Und dann gehen wir den Weg gemeinsam!

Es ist vor allem wichtig, mit einer positiven Grundhaltung an das Thema heranzugehen, denn ändern können wir daran ohnehin nichts mehr.

Du wirst sehen, dass es gar nicht sooo viele Dinge sind, an die wir künftig denken müssen.

Die erste Frage ist natürlich immer:

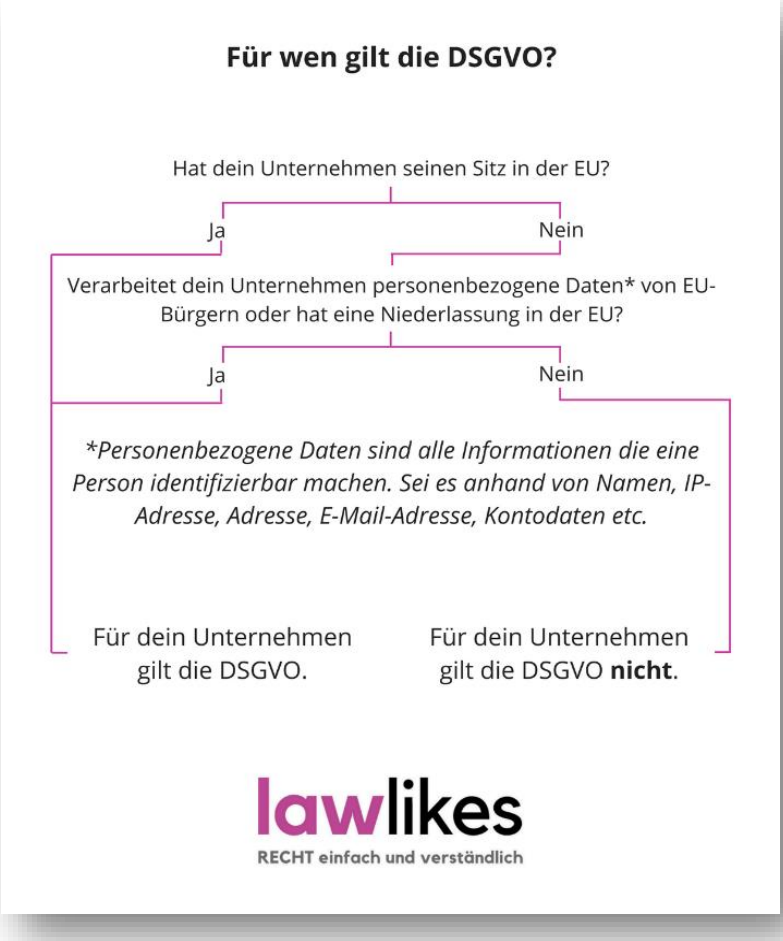
> „Was habe ich überhaupt mit der DSGVO zu tun? Es trifft doch sicher nur große Unternehmen, oder?“

Leider muss ich dir an dieser Stelle die Augen öffnen, denn die DSGVO trifft jeden, der in der EU personenbezogene Daten verarbeitet (Was das wiederum genau bedeutet, erkläre ich dir gleich noch!).

Selbst, wenn man schnell aus der EU wegziehen würde, nützt es nichts, da selbst dann, wenn man in einem sogenannten Nicht-EU-Drittland sitzt und dort seine Dienstleistungen oder Waren an Personen innerhalb der EU anbietet (und somit wieder personenbezogene Daten verarbeitet) ist man unmittelbar von der DSGVO betroffen.

Ihr braucht also DESWEGEN keine Auswanderung zu planen…

Weitere Info´s zur Frage, auf wen die DSGVO anwendbar ist, gibt es in unserer Info-Grafik:



So nun die wichtige und alles entscheidende Frage: **Was sind denn nun diese personenbezogenen Daten (PBD)?**

Du fragst dich jetzt bestimmt heimlich:

> „Vielleicht verarbeite ich ja keine PBD und bin damit raus aus dem Schneider?“

Das ist oft die leise Hoffnung von einigen Mandanten - leider traf es bislang nie zu…

Personenbezogene Daten sind nach **Art. 4 Nr. 1 DSGVO** alle Informationen, die sich auf eine natürliche Person beziehen oder zumindest auf eine solche beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. – Ähm, ja.

Im Klartext heißt das u.a.:

Namen

Alter

Geburtsdatum

Anschrift

Lichtbild

E-Mail-Adresse

Telefonnummer

Kreditkartendaten

Bankverbindung

IP-Adressen

Neben diesen „normalen“ Daten gibt es auch noch die „besonderen Kategorien von personenbezogenen Daten“ – und diese genießen auch einen besonderen Schutz.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert.

Beispiele:

Lichtbilder auf denen die ethnische Herkunft zu sehen ist (umstritten- aber um safe zu sein, gehen wir erstmal davon aus)

Angaben zum Gesundheitszustand

Gut, nun wissen also, was personenbezogene Daten sind. Was ist denn nun dieses **Verarbeiten**?

Art. 4 Ziff. 2 DSGVO definiert die Verarbeitung von Daten wie folgt:

„Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.”

Also bedeutet „Verarbeiten“ eigentlich alles 😉.

Du verarbeitest also z.B. personenbezogene Daten, wenn du

- Google Analytics oder Facebook Pixel einsetzt
- Einen E-Mail-Newsletter versendest
- Im Auftrag anderer mit personenbezogenen Daten zu tun hast, z.B. als Webdesigner, Fotograf oder virtuelle Assistentin
- Terminreservierungen telefonisch oder online anbietest
- Werbung an Kunden oder Interessenten versendest
- Eine Kundenkartei führst (egal, ob elektronisch oder auf Papier)
- Testimonials für deine Webseite oder deine digitalen Angebote nutzt
- Etc.

Ohne die Nutzung von personenbezogenen Daten würde dein Business also gar nicht funktionieren.

Auch Fotos von Kunden auf Social Media Plattformen oder der eigenen Website fallen unter die Verarbeitung personenbezogener Daten!

Jetzt geht es weiter mit dem wichtigsten Grundsatz, den du dir **UNBEDINGT** merken musst.

Personenbezogene Daten dürfen nicht verarbeitet werden!

Ich sehe die Fragezeichen in deinem Gesicht quasi vor mir. Aber es ist wichtig, dass du dir diesen Grundsatz einprägst. Denn er wird dich sensibilisieren, so dass du von alleine merken wirst, ob eine Verarbeitung von Daten in Ordnung ist oder eher nicht.

Also wir dürfen es grds. nicht – und jetzt kommt es: **außer** es liegen bestimmte Erlaubnistatbestände (ein klein wenig Juristendeutsch muss hier ja auch sein 😉)

Wir dürfen z.B. personenbezogene Daten verarbeiten, wenn wir sonst einen Vertrag nicht erfüllen können. Die Zusendung von Waren z.B. wäre ohne Adresse ebenso schwierig wie die Terminabstimmung mit einem Kunden ohne dabei seine Kontaktdaten zu nutzen.

Ebenso dürfen wir Daten verarbeiten und sogar die „besonderen“, wenn wir dafür eine wirksame Einwilligung eingeholt haben.

Wie eine solche Einwilligung aussehen muss, schauen wir uns anhand des Beispiels „E-Mail-Newsletter“ gleich genauer an.

Im Folgenden gehe ich auf einige für dich wichtige Beispiele genauer ein:

Die Online-Termin-Reservierung

Die Kundendaten sind dein wichtigstes Gut.

Für die Anwendung der DSGVO macht es keinen Unterschied, ob Kundendaten handschriftlich oder elektronisch abgelegt werden. Das Gesetz sieht vor, dass die Speicherung der Daten zweckmäßig erfolgt. Das bedeutet, dass die Daten auch nur so lange gespeichert werden dürfen, bis der Zweck erfüllt ist. Und auch nur für den Zweck, für den du ursprünglich die Daten eingesammelt hast.

Im Klartext: Wenn mich jemand über das Kontaktformular auf meiner Seite anschreibt, darf ich ihn natürlich über die angegebene E-Mail-Adresse kontaktieren um diese Anfrage zu bearbeiten - ich darf ihm jedoch nicht einfach Werbung zusenden.

Denn das wäre wiederum ein anderer Zweck und für diesen habe ich KEINE Erlaubnis.

Genauso ist es bei Online-Reservierungen. Wenn der Termin stattgefunden hat, müssten streng genommen die Daten anschließend gelöscht werden.

Damit man dieses nicht machen muss, sollte bei dem Termin eine Einwilligung eingeholt werden, um den Kunden in Zukunft auch telefonisch / per E-Mail etc. kontaktieren zu dürfen und zu diesem Zweck die Kontaktdaten weiterhin speichern zu dürfen.

Damit der Kunde aktiv seine Einwilligung erteilen kann, ist bei jeder Online-Reservierung eine Checkbox (so nennt man die Kästchen zum Ankreuzen oder Häkchen setzen) empfehlenswert.

Neben dem Link zu deinen Datenschutzbestimmungen, in welchen du definierst, wofür du die Daten speichern möchtest und für wie lange, sollte die Checkbox folgenden Wortlaut enthalten:

Ich möchte, dass meine Daten auch nach Ablauf des Termins weiterhin gespeichert werden, damit ich zukünftig von NAME kontaktiert werden kann.

Der E-Mail Newsletter

Falls du nun noch die E-Mail-Adresse des Kunden für künftige Newsletter speichern möchtest, so muss auch dieser Vorgang explizit eingewilligt werden. In einer **weiteren Checkbox** muss der Kunden durch aktives Anklicken dem Erhalt von Newslettern ausdrücklich zustimmen.

1. Einwilligung

Denn eine Einwilligung muss nach der DSGVO folgende Merkmal erfüllen:

A. Freiwillig

Also ohne Zwang. Wir dürfen also nicht sagen: „Du kannst mein Produkt nur kaufen, wenn du dich auch in den Newsletter einträgst."

Ebenso (wobei das heiß umstritten ist) sieht es mit unseren geliebten Freebies (so nennt man z.B. eBooks o.ä., die man kostenlos und sehr häufig nur gegen die Anmeldung im Newsletter herunterladen kann) aus. Denn auch hier gibt es Ansichten, die sagen, dass die Leute dann gezwungen werden, in den Newsletter zu kommen, um dann eine Leistung bzw. ein Produkt zu erhalten - obwohl diese Einwilligung in den Newsletter-Versand überhaupt nicht dafür erforderlich ist, dem Interessenten den Zugriff auf das Freebie zu geben.

Das heißt, wir verbinden 2 unterschiedliche Sachen fest miteinander („Koppeln" diese = daher nennt sich dieses streitbare Ding auch Koppelungsverbot), die eigentlich unabhängig voneinander stehen.

No. 1 (Grüner Risikobereich)

Um es ganz klar zu sagen: Die 100% Lösung sieht so aus, dass wir ein eBook, eine Checkliste o.ä. zur Verfügung stellen und die Landingpage so aufbauen, dass der Newsletter im Mittelpunkt steht und wir hier also Werbung für unseren Newsletter machen und erzählen, was die Abonnenten alles Tolles erwartet.

ABER: Es gibt eine gesonderte Checkbox, über die wir die Einwilligung für den Newsletter einholen. Die Checkliste bekomme ich auch ohne die Anmeldung.

Jetzt denken sicher viele:

„Na toll: Was soll das denn? Dann trägt sich ja niemand mehr in den Newsletter ein."

Ist das wirklich so? Überleg doch mal bitte, wann du das letzte Mal gezielt einen Newsletter abonniert hast. Ich weiß es noch für mich; denn das war bei Alexander Wiethaus von den E-Mail-Marketing Helden, denn ich wollte endlich Top-Inhalte und Tricks für das E-Mail-Marketing lernen. Und was soll ich sagen, ich habe mich total auf den 1. Newsletter gefreut, diesen richtiggehend aufgesogen und dann direkt weiterempfohlen – so wie hier 😉.

Alle anderen Newsletter, die sich so bei mir angesammelt haben, schaue ich ehrlich gesagt gar nicht mehr richtig an. Da war der erste Anreiz zu Beginn wirklich nur der Freebie und wenn dieser mich nicht überzeugt hatte, konnte es auch kein Newsletter hinterher. Und ich hätte auch sicher kein Produkt von diesem Anbieter gekauft.

Daher bin ich persönlich davon überzeugt, dass sich deine Interessenten auch freiwillig in den Newsletter eintragen – gerade, weil du dein tolles Freebie (Remember: Content stays King) einfach so anbietest - und eben nicht die Leute -ohne es klar zu sagen- in deinen Newsletter ziehst.

Für alle, denen das jetzt aber zu „Blumig" ist: Es gibt noch andere Ansichten zu dem Koppelungsverbot, die ich euch nicht vorenthalten möchte. Aber vorweg - KEINE dieser Varianten ist abmahnsicher – bis nicht ein Gericht darüber entschieden hat. Also Vorsicht und sicherheitshalber Rücklagen dafür bilden! 😉

No. 2 (Oranger Risikobereich)

Es gibt eine Ansicht, die sagt: „Wir stellen einfach eine Wahlmöglichkeit her."

Das heißt, man bietet auf einer Landingpage die Checkliste einmal gegen 9,99 € (Beispielspreis) und einmal gegen die Einwilligung, Werbe-E-Mails oder Anrufe zu bekommen, an. Hier ist wichtig, dass die Einwilligung ganz klar und so detailliert wie möglich beschrieben wird, damit der Interessent möglichst umfassend informiert wird was mit den Daten passiert; also wann und wie oft er zu welchen Themen und von welchem Unternehmen angeschrieben wird.

No. 3 (Oranger Risikobereich)

Wie No. 2, nur wird die Checkliste dabei nicht gegen Geld angeboten, sondern es werden Checkliste (Ware) gegen Daten (die wie Geld zu beurteilen sind) getauscht. So entsteht nach dieser Ansicht ein Vertragsverhältnis - das könnte man durch AGB oder Nutzungsbedingungen noch ausgestalten und somit wäre dann beides wirksam gekoppelt.

No. 4 (Oranger Risikobereich)

Wir verzichten auf eine Einwilligung und nehmen als Grundlage für die Verarbeitung der personenbezogenen Daten das sog. berechtigte Interesse nach Art. 6 Abs. 1 S.1 lit. f DSGVO. In dem dazu gehörigen Erwägungsgrund 47 wird das Direktmarketing als Beispiel für ein mögliches berechtigtes Interesse erwähnt. Ob darunter aber auch ein Newsletter fallen kann und wenn ja, unter welchen Voraussetzungen, kann man nicht mit absoluter Sicherheit sagen.

WICHTIG:

Falls ihr diese Variante trotz des bestehenden Risikos wählen möchtet, dann weist bitte in der 1. E-Mail ausdrücklich auf das jederzeitige Widerrufsrecht des Empfängershin. Das steht den Newsletter-Abonnenten immer auch ohne eine erklärte Einwilligung zu.

No.5 (Roter Risikobereich)

Alles bleibt wie es ist. Keine erweitere Information und die Interessenten werden weiter in den Newsletter bei Download des Freebies gezogen.

B. Für den bestimmten Fall

Eine pauschale Einwilligung in Form einer Blanko-Einwilligung ist unzulässig. Aus der Einwilligung muss erkennbar sein, welche personenbezogenen Daten zu welchem Zweck und von wem verarbeitet werden. Die Zwecke müssen möglichst genau bestimmt sein und dem Nutzer eine informierte Entscheidung ermöglichen.

Es ist erforderlich, klar anzugeben für welche Produkte oder Dienstleistungen man werben möchte bzw. um welche Themen es in dem Newsletter geht.

Soll der Newsletter an Bestandskunden nach § 7 Abs. 3 UWG geschickt werden, darf man auch die Formulierung „ähnliche wie von Ihnen erworbene Produkte/ Dienstleistungen“ verwenden.

C. Informiert

Hier geht es darum anzugeben, wie oft der Newsletter erscheinen wird. Wenn ihr es nicht genau wisst, gebt sicherheitshalber eine häufigere Sequenz an.

D. Unmissverständlich

Eine Opt-Out Möglichkeit ist nicht erlaubt. Der Interessent muss „tätig“ werden, durch aktives ankreuzen des Opt-Ins.

PUH so die Einwilligung haben wir nun schon mal.

Kurze Pause 😉 – denn es geht natürlich noch ein wenig weiter.

2. Freiwillige weitere Angaben

Nach dem Grundsatz der Datenminimierung darfst du außer der E-Mail-Adresse keine weiteren Daten abfragen. Natürlich kannst du den Vornamen als optionales Feld mit anbieten, damit du später den Empfänger direkt bzw. personalisiert ansprechen kannst.

Werden freiwillig weitere Daten angegeben, sind diese von der Einwilligung des Betroffenen mitumfasst.

3. Jederzeitige Widerrufsmöglichkeit

Es muss dem Newsletter-Empfänger jederzeit möglich sein, seinen Widerruf der Einwilligung zu erklären. In jedem Newsletter muss darauf hingewiesen werden, dass diese Widerrufsmöglichkeit besteht. Am besten wird also immer ein Link mitgesendet, über den dieser Widerruf möglich ist.

Jeder Widerruf muss dokumentiert und so verarbeitet werden, dass der Empfänger KEINE weitere E-Mail (mit Ausnahme der Abmeldebestätigung) mehr erhält.

Denn: Jede E-Mail nach einem Widerruf kann eine Abmahnung oder ein Bußgeld nach sich ziehen.

4. Verweis auf die Datenschutzerklärung und das Impressum

Dein Newsletter muss ein Impressum enthalten. Die Impressumspflicht im Newsletter ist im Telemediengesetz (TMG) in § 5 geregelt. Du musst deine Newsletter-Empfänger darüber aufklären, wer Absender des Newsletters ist (inkl. Anschrift). Hierfür kannst du den Footer im Newsletter verwenden. Dort sollte auch der Link zu deiner Datenschutzerklärung und zum Widerruf rein. Eine 3 in 1-Lösung sozusagen.

5. KEINE Werbung in der Bestätigungs-E-Mail zum Double-Opt-IN

Die Double-Opt-In E-Mails, also die Bestätigungsmails bei der Newsletter-Anmeldung, erhalten in der Regel sehr hohe Öffnungsraten und sind damit attraktiv für das Einbinden von Werbung. Dies ist allerdings nicht erlaubt, da der Nutzer zum Zeitpunkt zu dem er die E-Mail erhält, noch nicht dem Erhalt von Werbung zugestimmt hat. Das Unternehmenslogo darf jedoch in der E-Mail angezeigt werden.

6. KEINE Werbung in der Abmeldebestätigung

Hier gilt ebenfalls, dass auf Werbung komplett verzichtet werden muss.

7. Nachweisbarkeit der Einwilligung

Nach aktueller Rechtslage in Deutschland ist ein sogenanntes Double-Opt-In-Anmeldeverfahren (DOI) vorgesehen. Ein Empfänger bekommt bei der Anmeldung zum Newsletter eine Bestätigungsmail mit einem Bestätigungslink, bevor er aktiv in dem Newsletter-Verteiler aufgenommen wird. Erst wenn der Empfänger nun auch den Bestätigungslink in der Bestätigungsmail klickt, wird er aktiv in den Verteiler aufgenommen. Mit dem Double-Opt-In-Verfahren erfüllst du die Anforderung einer „ausdrücklichen Einwilligung“ bei der Newsletter-Anmeldung.

Die Einwilligung zum Newsletter solltest du in jedem Fall mit Text, Datum und Uhrzeit speichern, damit du diese im Ernstfall nachweisen kannst und die rechtliche Anforderung erfüllst.

8. Datenschutzerklärung

Damit sich deine Webseitenbesucher über die Verwendung ihrer personenbezogenen Daten rechtskonform informieren können, sollte deine Datenschutzerklärung einen Hinweis auf den Newsletter enthalten.

Hierbei solltest du beschreiben, was der Kunde von der Anmeldung zum Newsletter erwarten darf und was mit seinen Daten passiert.

Auch der Newsletter-Anbieter und die Rechtsgrundlage für die Datenverarbeitung (Das ist bei der Einwilligung Art. 6 Abs. 1 S. 1 lit. a) müssen genannt werden.

9. Auftragsverarbeitungsvertrag mit dem Newsletter-Anbieter

Du gibst die personenbezogenen Daten an einen Dritten zum Newsletter-Versand weiter. Der Versanddienstleister sollte nach den Datenschutzkriterien ausgewählt werden (siehe Art. 28ff. DSGVO).

Nach Art. 28ff. DSGVO bist du dazu verpflichtet, vor der Weitergabe personenbezogener Daten einen sogenannten Vertrag zur Auftragsverarbeitung abzuschließen. Diesen Vertrag muss dir der Newsletter-Anbieter zur Verfügung stellen.

In 12 Schritten zum DS_GVO konformen Newsletter 😉

- ☐ Die Einwilligung erfolgt freiwillig (Stichwort Koppelungsverbot)
- ☐ Die Einwilligung ist für den bestimmten Fall formuliert
- ☐ Der Interessent wird umfassend informiert (Sequenzen, Unternehmen, Inhalte)
- ☐ Der Interessent versteht, dass er hier eine Einwilligung zu einem Newsletter abgibt
- ☐ Freiwillige weitere Angaben – nur E-Mail-Adresse ist verpflichtend!
- ☐ Jederzeitige Widerrufsmöglichkeit per Link in jeder E-Mail
- ☐ Impressum in jeder E-Mail und Verlinkung auf die Datenschutzerklärung
- ☐ KEINE Werbung in der Bestätigungs-E-Mail zum Double-Opt-IN
- ☐ KEINE Werbung in der Abmeldebestätigung
- ☐ Double-Opt-In
- ☐ Aktuelle Datenschutzerklärung mit Passus E-Mail Newsletter
- ☐ Auftragsverarbeitungsvertrag vom E-Mail Newsletter Anbieter

lawlikes
RECHT einfach und verständlich

Bestandskunden sind doch etwas Schönes:

Nach Art. 7 Abs. 3 UWG, Art. 16 Abs. 2 ePrivacy-VO-E ist es – wenn die Voraussetzungen dieser Norm vorliegen zulässig OHNE Einwilligung E-Mails zu versenden! YEAH, endlich mal eine gute Nachricht!

Auch ein Opt-Out ist hier ausnahmsweise gestattet, da man von einem berechtigten Interesse, dass wir als Unternehmer an Direktwerbung haben, ausgeht (Art. 6 Abs. 1, S.1 lit. f). Das bedeutet, hier darf das Kästchen vor-angekreuzt sein.

Zudem rechne ein Bestandskunde damit, dass er Werbung zu ähnlichen wie den gekauften Produkten erhalte. Der Kunde sollte darüber aber in Kenntnis gesetzt werden und auch ohne erteilte Einwilligung auf sein jederzeitiges Widerrufsrecht hingewiesen werden.

In 8 Schritten zum DSGVO konformen Newsletter bei Bestandskunden 😉

- ☐ Bestandskunde nach § 7 Abs. 3 UWG. (Dann ist eine Einwilligung entbehrlich)
- ☐ Einwilligung ist auch mit Opt-Out bei der Bestellung möglich- aber klar kennzeichnen!
- ☐ Widerrufsmöglichkeit in 1. E-Mail bei Bestandskunden eingerichtet
- ☐ Inhalt des Newsletters für Bestandskunden nur für ähnliche Produkte
- ☐ Verweis auf die Datenschutzerklärung und das Impressum in jeder E-Mail
- ☐ KEINE Werbung in der Abmeldebestätigung
- ☐ Aktuelle Datenschutzerklärung mit Passus E-Mail Newsletter
- ☐ Auftragsverarbeitungsvertrag vom E-Mail Newsletter Anbieter

Gewinnspiele und Werbeeinwilligungen:

Gewinnspiele und Werbeeinwilligungen gegenüber Drittunternehmen sind ja auch sehr beliebt. Bitte zukünftig darauf achten, dass es natürlich möglich ist, eine Einwilligung für den Werbeversand auch für ein Drittunternehmen- welches natürlich benannt werden muss- einzuholen. Allerdings darf die Teilnahme am Gewinnspiel nicht an die Einwilligung in den Erhalt von Werbung geknüpft werden.

Genau – das Koppelungsverbot schlägt wieder zu. Auch hier gelten die oben angegebenen Hinweise und Möglichkeiten.

Auftragsdatenverarbeitung nach der DSGVO

Der Versand von Newslettern, die externe Lohn- und Gehaltsabrechnung, die externe Rechnungsbearbeitung / Buchhaltung, Papier- und Aktenvernichtung sowie die Vernichtung von Datenträgern durch externe Dienstleister sind Datenverarbeitungsvorgänge, die dem Datenschutzrecht unterliegen. Es ist eine sogenannte **Verarbeitung von Daten im Auftrag** und diese erfordert einen Vertrag. Sie muss den Anforderungen von Art. 28 DSGVO entsprechen. Außerdem müssen technische und organisatorische Maßnahmen nach Art. 32 DSGVO ergriffen werden, um den Schutz der Daten gewährleisten zu können.

Auch die Frage, wo der externe Dienstleister seinen **Sitz** hat, muss geklärt werden. Es macht datenschutzrechtlich einen Unterschied, ob die Datenverarbeitung bei den Anbietern und Dienstleistern außerhalb der EU (Drittstaat) oder im Geltungsbereich der EU-Datenschutzgrundverordnung erfolgt. Insbesondere gilt dies für die Datenverarbeitung in den USA oder durch US-Unternehmen. Die Verarbeitung in Drittstaaten ist nur rechtmäßig, wenn die Grundsätze der Datenverarbeitung in Drittstaaten berücksichtigt werden (Art. 44 DSGVO).

Von der Datenverarbeitung in Drittstaaten sind insbesondere Anbieter für den Newsletter-Versand betroffen.

lawlikes
RECHT einfach und verständlich

Speichern und Löschen von Daten nach DSGVO

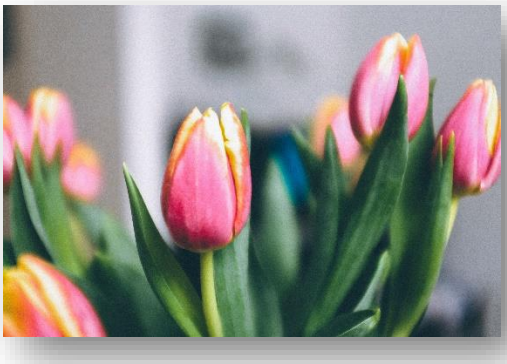
Personenbezogene Daten dürfen grundsätzlich nur solange verarbeitet werden, wie dies zur Erfüllung des Zweckes, zu dem sie erhoben wurden, notwendig ist. Sie sind anschließend zu löschen und dürfen somit nicht dauerhaft gespeichert werden.

Wenn du Produkte verkaufst, solltest du die Daten in jedem Fall für 24 Monate aufheben, da immer noch Gewährleistungsansprüche durch den Kunden geltend gemacht werden könnten.

Zudem musst du natürlich die steuerrechtlichen Aufbewahrungspflichten beachten- selbst wenn ein Kunde von dir verlangt, alle Daten zu löschen, gehen diese gesetzlichen Fristen vor. Wenn du dann die Daten nicht mehr brauchst, musst du diese natürlich komplett löschen.

Wo die Daten gesichert werden, in welchem Land der Server steht, ob die Kundenkartei sicher aufbewahrt wird oder die Frage danach, wer Zugriff auf die Daten hat muss geklärt und eigenverantwortlich dokumentiert werden, um für die Sicherheit der Daten zu sorgen. Falls dies kontrolliert wird, musst du all jene Informationen darlegen können. Es gilt, dass nur die Mitarbeiter, die zur Vertragserfüllung bestimmte Informationen benötigen, auch Zugriff auf diese Daten bekommen. Nicht jeder Mitarbeiter sollte Zugriff auf alle Daten jedes Kunden haben können und es sollte in jedem Fall eine Verschwiegenheitsvereinbarung getroffen werden.

Wenn du bis hierhin durchgehalten hast, dann hast du dir die Blumen redlich verdient. Jetzt folgt eine Checkliste, sodass du direkt loslegen kannst. Ich bin jetzt schon wirklich stolz auf dich, denn nach einer aktuellen Umfrage ist noch nicht mal jedes 3. Unternehmen dabei, sich gerade mit der DSGVO zu befassen - du gehörst also zu den Mutigen, die den Schritt gemacht haben!



Gehe die Punkte Schritt für Schritt durch und

wenn Fragen aufkommen, findet ihr mich hier: www.lawlikes.de

lawlikes
RECHT einfach und verständlich

Checkliste

☐ **Bestandsaufnahme**
Verschaffe dir einen Überblick, wo du überall personenbezogene Daten verarbeitest – denk daran, verarbeiten bedeutet nicht nur AKTIV Daten irgendwo einzupflegen, sondern auch wenn automatisch -wie z.B. bei Google Analytics- Daten verarbeitet bzw. weitergegeben werden.

Stell dir dazu vor, du hättest Interesse an deiner eigenen Dienstleistung – wie wird man dein Kunde? Was machst du, wenn man Kunde ist - welche Daten benötigst du dann und wie kommen die Daten zu dir? Der „Weg der Daten" ist also wichtig!

Prüfe, ob du ein Verzeichnis von Verarbeitungstätigkeiten benötigst und beginne dann damit, ein solches Verzeichnis anzulegen!

☐ **Webseite**
Ist deine Webseite bereits SSL oder TLS verschlüsselt?

Ist dein Kontaktformular verschlüsselt?

Hast du eine individuelle Datenschutzerklärung, die alle Datenverarbeitungen, Cookies und Plugins auf deiner Webseite berücksichtigt?

Um herauszufinden, was du alles auf der Webseite einsetzt, solltest du deinen Webdesigner fragen oder dir mit einem einfachen Tool wie z.B. Ghostery selber einen ersten Überblick verschaffen!

Hast du eine Opt-Out-Möglichkeit für Google Analytics und für den Facebook Pixel eingerichtet?

Hast du ein vollständiges Impressum?

☐ **Auftragsverarbeiter und die zugehörigen Verträge**
Hast du Auftragsverarbeitungsverträge mit deinem Webseiten-Hoster, mit deinem Buchungstoolanbieter, mit deinem Newsletter-Anbieter, mit deiner virtuellen Assistentin, mit Google-Analytics u.s.w.?

☐ **Du bist selber Auftragsverarbeiter**
Hast du einen Auftragsverarbeitungsvertrag, den du deinen Kunden zur Verfügung stellen kannst? Hast du selbst wiederum Verträge mit Subunternehmern, die dir bei deiner Leistungsausübung gegenüber dem Kunden helfen? Hat dein Kunde eingewilligt, dass du diese Subunternehmer einbinden kannst?

Hast du eine Verschwiegenheitsverpflichtung gegenüber deinem Kunden erstellt? Hast du bereits ein Verarbeitungsverzeichnis für Auftragsverarbeiter erstellt?

☐ **Newsletter**
Dein Newsletter ist optimal eingerichtet?! (Vorgaben siehe oben)

☐ **Einwilligungen deiner Kunden**
Hast du hast Einwilligungsformulare für deine Kunden erstellt? (Vorgaben siehe oben)
Hast du bestehende Formulare an die neue Rechtslage angepasst?
Hast du eine Verschwiegenheitserklärung mit allen Mitarbeitern (auch freien Mitarbeitern, Praktikanten etc.), die personenbezogene Daten verarbeiten oder damit in Berührung kommen?

☐ **Einwilligung**
Hast du ein Einwilligungsformular, dass es dir erlaubt, deine Kunden rechtssicher anzusprechen?
Das Formular muss sehr detailliert sein und mehrere Einwilligungen enthalten: z.B. einmal, um Kontakt per Whats-App aufzunehmen und gesondert, um Bilder als Testimonial zu verwenden.

☐ **Formulare**
Überprüfe die bislang verwendeten Formulare (z.B. Aufklärungs- und Einwilligungsbögen sowie Zustimmungserklärungen in AGB und auf deinen Webseiten).
Achte vor allem darauf, dass du nur die notwendigsten Daten abfragst. Wenn du Gesundheitsdaten oder andere besonders sensible Daten abfragst, lass dir die Verwendung dieser besonderen personenbezogenen Daten durch eine Einwilligung genehmigen.

☐ **Datenlöschung**
Wenn du die Kundendaten nicht mehr benötigst, solltest du diese löschen.

Du solltest, wenn ein Kunde ein Produkt gekauft hat, die Daten auch zum Kauf für 24 Monate aufheben. Denn solange könnte er noch einen Gewährleistungsanspruch geltend machen.

Die Rechnungen und alles was du für die Buchhaltung benötigst, musst du 10 Jahre aufbewahren.

☐ **Datensicherheit / Technische und organisatorische Maßnahmen (TOM)**
Hast du ein individuelles Datensicherheitskonzept, in dem u.a. die folgenden Punkte geregelt sind: Datensicherung-/Backup, Passwortkonzept, Berechtigungskonzept für Software, Notfall- und Wiederanlaufplan bei Verlust von Hardware und/oder Daten,

Zutrittskonzepte für Büro/Homeoffice, Umgang mit Internet, E-Mail und eigener Hardware von Mitarbeitern etc.?

☐ **Rechte der Betroffenen / Zusammenarbeit mit Behörden**
Hast du organisiert, was wie zu tun ist, wenn betroffene Personen eine Auskunft über die Verwendung ihrer Daten verlangen?

Weißt du, welche Maßnahmen du einleiten musst, wenn eine Datenpanne passiert ist und an wen du dich dann zu wenden hast?

So, das war mal ein Überblick zu den zentralen DSGVO-Themen für Online-lastige Geschäftsmodelle, wie deines vielleicht eins ist.

Sei mal ehrlich: Da war bestimmt einiges dabei, was für auch dich relevant ist, oder?

Wir hoffen jedenfalls sehr, dass dir unsere Checkliste bei der Orientierung geholfen hat!

Unser Ziel war es, dich für die wichtigen Themen zu sensibilisieren!

Du siehst: es gibt keinen Grund dafür, verunsichert zu sein oder Ängste zu haben – denn mit einem guten Plan ist die Umsetzung schnell auf den Weg gebracht!

Wenn du mehr Details dazu wissen möchtest und um weitere Informationen und interessante Angebote zur DSGVO zu erhalten, kannst du dich hier für unseren E-Mail-Newsletter eintragen. Bereits in den nächsten Tagen geht es dort direkt weiter mit Tipps und Hilfen rund um das neue Datenschutzgesetz.

Ich freue mich, wenn ich hiermit schonmal ein wenig zur Aufklärung beitragen konnte!

Viele Grüße

Deine Sabrina Keese-Haufs