SASSENBACH
ADVERTISING

Wichtige Hinweise zur Geltung der Datenschutz-Grundverordnung (DSGVO) ab dem 25.05.2018

Liebe Harley Händler,

ab dem 25.05.2018 gilt europaweit die DSGVO. Praktisch ändert sich für Sie erst mal nichts. Die Sassenbach GmbH stellt Ihnen nach wie vor das DMS-Newslettertool für den Versand von E-Mail-Newslettern an Ihre Endkunden zur Verfügung. In diesem Zusammenhang verarbeiten wir personenbezogene Daten Ihrer Endkunden streng nach Ihren Vorgaben und Ihren Weisungen als sog. Auftragsverarbeiter gemäß Art. 28 DSGVO. Soweit Sie uns ausdrücklich damit beauftragt haben, versenden wir in Ihrem Auftrag auch postalische Nachrichten an Ihre Endkunden.

Wir haben Ihnen in den letzten Wochen auch schon ein Paket geschickt, in dem Sie eine sog. „Auftragsverarbeitungs-Vereinbarung“ gemäß den gesetzlichen Vorgaben finden, die Sie uns gerne noch unterzeichnet zurückschicken können, sofern noch nicht geschehen. Wir möchten Ihnen aber dennoch im Folgenden die wichtigsten Richtlinien zur Datenverarbeitung durch uns zusammenfassen.

Melden Sie Sich jederzeit gerne bei uns, wenn Sie noch Rückfragen haben.

Ihr Sassenbach-Team

Sassenbach GmbH · Drygalski-Allee 25 · 81477 München · Telefon 0049. (0)89. 452 455-0 · Fax 0049. (0)89. 452 455-200
Büro Köln: Hohe Straße 128–132 · 50667 Köln · Telefon 0049. (0)221. 569 606-0 · Fax 0049. (0)221. 569 606-26
Geschäftsführer: Thomas Sassenbach, Peter Metz · Sitz: München · HRB 140975 Amtsgericht München · St.-Nr. 143/177/90008 · USt-IdNr. DE813356232
www.sassenbach.de

Richtlinien zur Datenverarbeitung durch die Sassenbach GmbH als Auftragsverarbeiter gemäß Art. 28 DSGVO

Wem gehören die Daten?
Alle Daten von Endkunden, die im Rahmen der Nutzung unseres DMS-Newslettertools verarbeitet werden, um Ihren Endkunden Newsletter versenden zu können, gehören einzig und alleine Ihnen.
Sassenbach wird lediglich als Auftragsverarbeiter bzw. Dienstleister in Ihrem Auftrag tätig, um Sie technisch bei dem Versand zu unterstützen. Das heißt, verantwortlich z. B. für die Einholung erforderlicher Einwilligungen bei Ihren Endkunden – gleichgültig, ob Sie Einwilligungen per „Offline"-Formular einholen oder im Wege des im Tool vorgesehenen Double-Opt-in-Verfahrens bei elektronischen Anmeldungen – bleibt der jeweilige Händler.

Welche Daten werden von Sassenbach verarbeitet?
Wir verarbeiten in Ihrem Auftrag diejenigen Daten, die Sie uns bereitstellen. In der Regel beschränkt sich dies auf den Vor- und Nachnamen sowie die E-Mail-Adressen Ihrer Endkunden, denen Sie E-Mail-Newsletter senden möchten. Wenn Sie uns auch mit dem Versand postalischer Werbung beauftragt haben, verarbeiten wir zusätzlich die von Ihnen zu diesem Zweck zur Verfügung gestellten postalischen Anschriften Ihrer Endkunden.

Zu welchen Zwecken genau werden die Daten von Sassenbach verarbeitet?
Ausschließlich auf Ihre Weisung zum Versand von E-Mail-Newslettern und – nur soweit Sie das beauftragt haben – zum Versand postalischer Werbung an Ihre Endkunden. Sassenbach verarbeitet die Daten natürlich nicht zu eigenen Zwecken und insbesondere nicht dazu, Ihren Endkunden eigene Werbung von Sassenbach oder gar Dritten zu zuzuschicken.
Sassenbach darf die Daten, die in Ihrem Auftrag verarbeitet werden, auch nicht eigenmächtig, sondern nur nach dokumentierter Weisung von Ihnen berichtigen, löschen oder deren Verarbeitung einschränken.

Müssen wir unsere Kunden in unseren Datenschutzerklärungen auf der Website über den Einsatz von Sassenbach als Dienstleister informieren?

Die DSGVO verpflichtet Verantwortliche dazu, ihre Kunden auch über „Empfänger" bzw. Dienstleister zu unterrichten. Da beim Newsletterversand in eingeschränktem Umfang (aber nicht personenbezogen) ein Tracking z. B. bzgl. der Öffnung der Newsletter stattfindet, empfehlen wir Ihnen, in Ihre Datenschutzerklärung folgenden Hinweis aufzunehmen:

„Für den Versand eines von Ihnen bestellten Newsletters an Sie setzen wir ein Newsletter-Versandtool unseres Dienstleisters Sassenbach GmbH, München/Deutschland ein. Für die Anmeldung zu unserem Newsletter verwenden wir das sog. Double-Opt-in-Verfahren. Das heißt, dass wir Ihnen nach Ihrer Anmeldung eine E-Mail an die angegebene E-Mail-Adresse senden, in welcher wir Sie um Bestätigung bitten, dass Sie den Versand des Newsletters wünschen. Zum Zweck der Anmeldung zum Newsletter werden Sie hierfür auf eine externe Website weitergeleitet. E-Mail-Adressen unserer Newsletterabonnenten sowie die zugehörigen zur Protokollierung/ zum Nachweis der Anmeldung zum Newsletter erforderlichen Anmeldedaten werden dabei auf Servern ausschließlich innerhalb der Europäischen Union/des Europäischen Wirtschaftsraums gespeichert. Diese Daten werden ausschließlich in unserem Auftrag zum Versand der Newsletter und zur Speicherung der Anmeldedaten im Tool verarbeitet, nicht für andere Zwecke und insbesondere nicht z. B. für einen Versand eigener E-Mail-Nachrichten durch den Dienstleister an Sie. Rechtsgrundlage für den Einsatz des Dienstleisters ist Art. 28 DSGVO (Verarbeitung durch einen Auftragsverarbeiter).

Die Newsletter enthalten einen „web-beacon", das heißt eine pixelgroße Datei, die es uns ermöglicht, auf anonymer Basis auszuwerten, ob und wann ein Newsletter geöffnet wurde und welche Links im Newsletter angeklickt wurden. Damit können wir aggregierte Statistiken z. B. über die Gesamtzahl der geöffneten Newsletter aller Abonnenten erstellen. In diesem Rahmen werden technische Informationen wie Informationen zu Ihrem Browser und Ihrem System, jedoch keine personenbezogenen Daten und auch nicht Ihre IP-Adresse gespeichert bzw. verarbeitet. Dabei ist es uns insbesondere nicht möglich, nachzuvollziehen, ob Sie persönlich den Newsletter geöffnet haben oder einen Link angeklickt haben. Wir nutzen die statistischen Auswertungen, um unseren Newsletter kontinuierlich optimieren zu können. Diese Analyse erfolgt in unserem Auftrag durch unseren Dienstleister Sassenbach GmbH, München/Deutschland. Rechtsgrundlage für die Analyse der Newsletternutzung ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO (Verarbeitung ist zur Wahrung berechtigter Interessen erforderlich). Wenn Sie keine Analyse der Newsletternutzung wünschen, empfehlen wir Ihnen, sich vom Newsletter durch Klick auf den in jedem Newsletter enthaltenen Abmeldelink abzumelden."

Welche Pflichten hat die Sassenbach GmbH als Auftragsverarbeiter?
Als Auftragsverarbeiter erfüllen wir unsere gesetzlichen Pflichten gemäß Art. 28 bis 33 DSGVO, insbesondere folgende Vorgaben:

- Wir haben einen externen Datenschutzbeauftragten bestellt (Herrn Bassam Saleh, Straßer Ventroni Deubzer Freytag & Jäger Rechtsanwälte, Oberanger 30, 80331 München) bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
- Wir wahren selbstverständlich die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b) 29, 32 Abs. 4 DSGVO. Wir setzen bei der Durchführung unserer Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
- Wir haben alle für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c) 32 DSGVO umgesetzt und halten diese ein (Einzelheiten siehe unten).
- Wir werden Sie unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf unsere Leistungen Ihnen gegenüber beziehen, unterrichten.
- Soweit Sie Ihrerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt sind, werden wir Sie nach besten Kräften und in angemessenem Umfang unterstützen.
- Wir kontrollieren regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung stets im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

Kann die Einhaltung der Verpflichtungen von Sassenbach kontrolliert werden?
Wir stellen sicher, dass Sie sich von der Einhaltung unserer Pflichten überzeugen können. Wir geben Ihnen auf Anfrage alle erforderlichen Auskünfte und ermöglichen Ihnen nach vorheriger Anmeldung selbstverständlich auch Vor-Ort-Kontrollen in angemessenem Umfang.

Setzt Sassenbach Subunternehmer ein?
Für den Versand der E-Mail-Newsletter setzen wir keine Subunternehmer bzw. weitere Dienstleister ein. Wenn Sie uns gleichzeitig auch mit dem Versand postalischer Werbung beauftragt haben, setzen wir in den betreffenden Ländern Deutschland, Österreich und Schweiz Druckdienstleister und Lettershops ein, mit denen wir ebenfalls Auftragsverarbeitungs-Verträge abgeschlossen haben. Auch unsere Subunternehmer dürfen die Daten nur streng zweckgebunden für die Erfüllung der vertraglichen Leistungen verarbeiten, nicht für andere bzw. eigene Zwecke.

Wo werden die Daten gespeichert?
Die Daten werden ausschließlich innerhalb der EU/des EWR gespeichert und verarbeitet. Eine Verarbeitung außerhalb der EU/des EWR findet nicht statt.

Wie schützt Sassenbach die Daten?
Um die Daten bestmöglich zu schützen, haben wir auf Basis der gesetzlichen Vorgaben des Art. 32 DSGVO folgende technische und organisatorische Maßnahmen implementiert. Wir werden auch bei erforderlich werdenden Anpassungen der unten getroffenen Maßnahmen sicherstellen, dass diese das getroffene Schutzniveau nicht unterschreiten:

I. Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Die Räumlichkeiten sind durch eine Alarmanlage gesichert
- Die Räumlichkeiten verfügen über ein manuelles Schließsystem
- Die Räumlichkeiten sind zusätzlich durch Sicherheitsschlösser abgesichert
- Die Räumlichkeiten verfügen über ein Chipkarten-/Transponder-Schließsystem
- Für den Zugang für Mitarbeiter ist eine Schlüsselregelung mit protokollierter und eingeschränkter Schlüsselaus- und -rückgabe implementiert
- Besuchern/Dritten ist ein Zutritt zu den Räumlichkeiten nur nach vorheriger Anmeldung während der Geschäftszeiten möglich
- Besucher/Dritte werden von dem jeweiligen Mitarbeiter in Empfang genommen und halten sich nicht unbeaufsichtigt bzw. alleine in Räumlichkeiten auf
- Das Reinigungspersonal wurde und wird im Falle eines Ersatzes sorgfältig ausgewählt

2. Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Sichere Passwortvergabe implementiert
- Strenge Passwortrichtlinie für Mitarbeiter (insbesondere zu Länge, Passwortstärke etc.)
- Erfordernis und Umsetzung regelmäßiger Passwortänderungen durch Mitarbeiter
- IT-Sicherheitsrichtlinie mit verbindlichen Regelungen zum sicheren Arbeitsplatz/PC
- Regelmäßige Änderung von WLAN-Kennwörtern
- Authentifikation mit Benutzername/Passwort an Datenverarbeitungssystemen zwingend erforderlich
- Intrusion-Detection-Systeme kommen zum Einsatz

- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz von VPN-Technologie
- Verschlüsselung mobiler PCs/Laptops

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Verschlüsselung mobiler PCs/Laptops
- Anzahl der System-Administratoren auf das „Notwendigste" reduziert
- Verwaltung der Rechte nur durch die System-Administratoren
- Sichere Passwortvergabe implementiert
- Strenge Passwortrichtlinie für Mitarbeiter (insbesondere zu Länge, Passwortstärke etc.)
- Erfordernis und Umsetzung regelmäßiger Passwortänderungen durch Mitarbeiter
- IT-Sicherheitsrichtlinie mit verbindlichen Regelungen zur sicheren Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel/Zertifizierungen bzw. verbindlicher Einhaltung einschlägiger DIN-Normen)
- Soweit Datenträger einer Vernichtung zugeführt werden müssen, erfolgt eine sorgfältige Auswahl von Dienstleistern mit Verpflichtung zur Protokollierung der Vernichtung

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Soweit die Verarbeitung pseudonymisierter Daten erforderlich oder zweckmäßig ist: Trennung der Zuordnungsdatei von den restlichen Datensätzen.

II. Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Einsatz von E-Mail-Verschlüsselung (Einsatz des Programms PGP „Pretty Good Privacy“)
- Verschlüsselung mobiler Datenträger
- Einsatz von verschlüsselten, passwortgeschützten ZIP-Dateien
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form, soweit zweckmäßig/erforderlich
- IT-Sicherheitsrichtlinie mit Regelungen zur elektronischen Übertragung/zum Transport von Datenträgern
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten (Logfiles)
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

III. Sicherstellung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

Maßnahmen, die gewährleisten, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Anlagen, Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind und Daten vor zufälliger Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Back-up- und Recovery-Konzepts
- Notfallplan
- Serverräume befinden sich nicht unter sanitären Anlagen

IV. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Effektive und sichere Vertragsgestaltung
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit), Durchführung von Recherchen zum Auftragnehmer
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen, insbesondere dessen technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO
- Klauseln zur Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit
- Prüfung, ob der Auftragnehmer Subunternehmer einsetzt, und Prüfung der Orte der Datenverarbeitung (insbesondere im Hinblick auf Speicherung der Daten innerhalb der EU/des EWR)

- Prüfung bzgl. Bestellung bzw. Bestellungspflicht eines Datenschutzbeauftragten beim Auftragnehmer, soweit gesetzlich erforderlich. Nennung von Ansprechpartnern des Auftragnehmers zur Datenverarbeitung, soweit keine gesetzliche Pflicht zur Bestellung eines Datenschutzbeauftragten besteht
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags durch Klauseln, die eine automatische Löschung nach Beendigung des Auftrags vorsehen einschl. Kontrolle der Löschung der Daten
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Vertragsstrafen bei Verstößen
- Abschluss von Vertraulichkeitsvereinbarungen mit Regelungen zum Datenschutz/zur Datensicherheit, soweit es sich nicht um eine Auftragsverarbeitung gemäß Art. 28 DSGVO handelt

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen (Art. 32 Abs. 1 lit. d) DSGVO)

- Regelmäßige Revision und Prüfung der implementierten Maßnahmen, mindestens einmal jährlich sowie anlassbezogen, z. B. bei neuen Prozessen/neuen Anschaffungen
- Regelmäßige Information und Austausch zwischen Geschäftsführung, System-Administratoren und Datenschutzbeauftragtem über neu auftretende Schwachstellen und andere Risikofaktoren
- Laufende und regelmäßige Abstimmung zwischen Geschäftsführung, System-Administratoren und Datenschutzbeauftragtem
- Datenschutzschulungen für Mitarbeiter (z. B. anlassbezogen bei Gesetzesänderungen wie der DSGVO)