



Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU
Datenschutz-Grundverordnung
(AV-Vertrag)

zwischen

und

SchokoFoto Marion Franz e.K.

Industriestr. 25

22880 Wedel

vertreten durch

vertreten durch

Marion Franz

im Folgenden: **Auftraggeberin**

im Folgenden: **Auftragnehmerin**

1. Gegenstand und Dauer der Verarbeitung

- (1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch die Auftragnehmerin: Druck auf weiße Schokolade und Fotoprälinen mit Lebensmittelfarben. Versand der Aufträge. Der Versand erfolgt im Namen der Auftraggeberin.
- (2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

2. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

2.1 Art und Zweck der Verarbeitung

- (1) Individualisierung von Schokoladen und Fotoprälinen bzw. Logoprälinen mit den Daten der Kunden der Auftraggeberin.
- (2) Bei Erfüllung dieser Dienstleistung werden die von der Auftraggeberin übertragenen persönlichen Daten ihrer Kunden verwendet.
- (3) Der Versand erfolgt nach Angaben der übertragenen Lieferadressen des Auftraggeberin.

2.2 Art der Daten

Es werden folgende Daten von der Auftraggeberin verarbeitet:

- Art des Produktes
- Druckdaten der Kunden der Auftraggeberin
- Menge und Sorte der zu bedruckenden Produkte
- Liefertermin
- persönliche Daten für den Versand

2.2.1 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Die Auftraggeberin und deren Mitarbeiter, falls vorhanden
- Mitarbeiter von SchokoFoto Marion Franz e.K.
- Logistikunternehmen

3. Pflichten des Auftragnehmers

- (1) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie von der Auftraggeberin angewiesen, es sei denn, die Auftragnehmerin ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für sie bestehen, teilt die Auftragnehmerin diese der Auftraggeberin vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihr gesetzlich verboten. Die Auftragnehmerin verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Sie beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) Die Auftragnehmerin verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (5) Im Zusammenhang mit der beauftragten Verarbeitung hat die Auftragnehmerin der Auftraggeberin bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und der Auftraggeberin auf Anforderung unverzüglich zuzuleiten.
- (6) Wird die Auftraggeberin durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihr gegenüber Rechte geltend, verpflichtet sich die Auftragnehmerin der Auftraggeberin im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (7) Auskünfte an Dritte oder den Betroffenen darf die Auftragnehmerin nur nach vorheriger Zustimmung durch die Auftraggeberin erteilen. Direkt an ihr gerichtete Anfragen wird sie unverzüglich an die Auftraggeberin weiterleiten.
- (8) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zwecke der direkten Kontaktaufnahme mitgeteilt.
- (9) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

4. Technische und organisatorische Maßnahmen

- (1) Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 1 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- (2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.
- (3) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der

Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

5. Regelungen zur Speicherung und Löschung von Daten

- (1) Die Auftragnehmerin speichert die Druckdaten maximal drei Monate ab Ausführung des Auftrages. Anschließend löscht sie die Daten automatisch und ohne dass es einer Aufforderung durch die Auftraggeberin bedarf.
- (2) Die Auftragnehmerin hat den Nachweis der ordnungsgemäßen Vernichtung zu führen.
- (3) Den entsprechenden Weisungen der Auftraggeberin wird die Auftragnehmerin jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

6. Unterauftragsverhältnisse

- (1) Für den Gegenstand dieses Vertrages sind keine Unterauftragnehmer von der Auftragnehmerin vorgesehen.
- (2) Unterauftragnehmer hat die Auftragnehmerin nur bei gewünschten Zusatzleistungen wie: Individualisierte Verpackungen oder konventionellen Druckdienstleistungen.
- (3) Die Beauftragung von Subunternehmern für diese Zusatzleistungen ist von der Auftraggeberin mit dem Erhalt der Auftragsbestätigung bestätigt.
- (4) Die Verantwortlichkeiten der Auftragnehmerin und der Subunternehmer sind eindeutig voneinander abzugrenzen.
- (5) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Die Auftraggeberin erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmerin und Subunternehmer.

7. Rechte und Pflichten der Auftraggeberin

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein die Auftraggeberin verantwortlich.
- (2) Die Auftraggeberin erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird die Auftraggeberin unverzüglich dokumentiert bestätigen.
- (3) Die Auftraggeberin informiert die Auftragnehmerin unverzüglich, wenn sie Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Die Auftraggeberin ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen bei der Auftragnehmerin in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist von der Auftragnehmerin soweit erforderlich Zutritt und Einblick zu ermöglichen. Die Auftragnehmerin ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
- (5) Kontrollen bei der Auftragnehmerin haben ohne vermeidbare Störungen ihres Geschäftsbetriebs zu erfolgen. Soweit nicht aus von der Auftraggeberin zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten der Auftragnehmerin, sowie nicht häufiger als alle 12 Monate statt. Soweit die Auftragnehmerin den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8. Mitteilungspflichten

- (1) Die Auftragnehmerin teilt der Auftraggeberin Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis der Auftragnehmerin vom relevanten Ereignis an eine von der Auftraggeberin benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
-

- a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstöße der Auftragnehmerin oder der bei ihr beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- (3) Die Auftragnehmerin informiert die Auftraggeberin unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Die Auftragnehmerin sichert zu, die Auftraggeberin bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9. Weisungen

- (1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenen-Rechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.
- (2) Die Auftraggeberin behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (3) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen.
- (4) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragsverarbeiterin unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.
- (5) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.
- (6) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

10. Beendigung des Auftrags

- (1) Bei Beendigung des Auftragsverhältnisses (siehe Absatz 2) oder jederzeit auf Verlangen der Auftraggeberin hat die Auftragnehmerin die im Auftrag verarbeiteten Druck- und Versanddaten zu löschen. Soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

- (2) Die Auftragnehmerin speichert die Druckdaten maximal drei Monate ab Ausführung des Auftrages. Anschließend löscht sie die Daten automatisch und ohne dass es einer Aufforderung durch die Auftraggeberin bedarf.
- (3) Die Auftragnehmerin hat den Nachweis der ordnungsgemäßen Vernichtung zu führen.
- (4) Die Auftraggeberin kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die Auftragnehmerin einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeberin aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

11. Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin der Auftraggeberin unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform erforderlich, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.
- (4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

Anlage 1 – technische und organisatorische Maßnahmen

Name und Kontaktdaten des Datenschutzbeauftragten der Auftragnehmerin:

SchokoFoto Marion Franz e.K. Marion Franz
Industriestr. 25
22880 Wedel

techn. Unterstützung von: Stephan Bröker; s.broeker@schokofoto.de
Befreit vom Datenschutzbeauftragten nach § 4f Abs. 1 Satz 3 BDSG.

Zuständige Datenschutz-Behörde für Auftragnehmerin:

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
(Anstalt des öffentlichen Rechts)
<https://www.datenschutzzentrum.de>

(1) Zutrittskontrolle

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

- Lichtschranken / Bewegungsmelder
- Schlüsselregelungen (Schlüsselausgabe etc.)
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal (Angestellte von SchokoFoto)

(2) Zugangskontrolle

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

- Vergabe von Benutzerrechten
- Vorgaben für sichere Passwörter
- Authentifikation mit Benutzername/Passwort
- Einsatz von individuellen Benutzernamen
- Zuordnung von Benutzerprofilen zu ITSystemen
- Firewall

(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.

- Erstellen eines Berechtigungskonzepts
- Sparsamer Umgang mit Admin-Rechten
- Protokollierung von Zugriffen auf
- Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
Verwaltung der Rechte durch Systemadministrator
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall

(4) Weitergabekontrolle

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

- Es erfolgt keine Weitergabe der Daten. Durch die vertragsbedingte Löschung nach 3 Monaten erfolgt auch keine Speicherung auf externen Medien.
- Backups werden ebenfalls nach 3 Monaten gelöscht.