

Vertrag

Auftragsdatenverarbeitung

(Rechtsgrundlage Vertragserfüllung Art. 6 Abs. 1 lit. b DSGVO)

zwischen

- Auftraggeber -

und

Lucky-Pet Handels- und Produktionsgesellschaft mbH
Sandkamp 7
23843 Bad Oldesloe

- Auftragnehmer -

Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsdatenverarbeitung i.S.d. § 11 BDSG bzw. den Vertrag i.S.d. Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3) Soweit das BDSG hier im Vertrag erwähnt wird, sind diese Erwähnungen nur noch bis zum Ablauf des 24.05.2018 zu berücksichtigen. Ab dem 25.05.2018 gelten dann die insoweit vorgenommenen Erwähnungen der DSGVO in diesem Vertrag.

Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Im Rahmen der einer Beziehung versenden wir Waren in Ihrem Auftrag an Kunden Ihres Unternehmens. Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Lieferadresse (Ihres Kunden):

- Vor- und Zuname
- Anschrift (Straße, Hausnummer, Postleitzahl, Ort, Land)

Produktdaten (Ihrer Kundenbestellung):

- Anzahl gekaufter Produkte
- Bezeichnung gekaufter Produkte

Kreis der von der Datenverarbeitung Betroffenen:

Kunden, Auftraggeber, Mitarbeiter der Fa. Lucky-Pet, Versanddienstleister

Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist verantwortliche Stelle (§ 3 Abs. 7 BDSG) bzw. Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(2) Der Auftraggeber ist als verantwortliche Stelle / Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

(4) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen.

Weisungen können schriftlich, per Fax, per E-Mail, mündlich erfolgen.

Der Auftraggeber soll mündliche Weisungen, sofern diese in diesem Vertrag für Weisungen zulässig sind, unverzüglich in Textform (z.B. Fax, E-Mail) gegenüber dem Auftragnehmer bestätigen.

(5) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(6) Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind:

Vertreter des o.g. Auftraggebers. Eine Prüfung der Weisungsbefugnis seitens des Auftragnehmers erfolgt nicht.

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

(7) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(8) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach § 42a BDSG, § 15a TMG, § 109a TKG oder Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(2) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

(3) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bestellt bzw. nach Art. 37 DSGVO benannt hat. Die Pflicht zur Bestätigung kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

(4) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(5) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durch-

führung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(7) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach § 38 BDSG oder Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(8) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

besondere Arten personenbezogener Daten (§ 3 Absatz 9 BDSG / Art. 9 DSGVO) oder
personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder (auch i.S.v. Art. 10 DSGVO)
personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalles/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

Dem Auftragnehmer ist bekannt, dass für den Auftraggeber ab dem 25.05.2018 eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

(9) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(10) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

(11) An der Erstellung der Verfahrensverzeichnisse bzw. Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(12) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur

Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-35 DSGVO genannten Pflichten.

(13) Der Auftragnehmer soll dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

Weisungsempfangsberechtigte Personen des Auftragnehmers sind:

- Datenschutzbeauftragter
- Geschäftsführung
- Mitarbeiter des Bereichs: Kundendienst
- Mitarbeiter des Bereichs: Versand / Logistik

Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. § 38 BDSG oder Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der „Anlage 1“ zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach § 9 BDSG bzw. ab dem 25.05.2018 die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen

zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bzw. Art. 37 DSGVO bestellt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Subunternehmer bestellt ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Der Auftragnehmer hat mit dem Subunternehmer einen Auftragsdatenverarbeitungsvertrag zu schließen, der den Voraussetzungen des § 11 BDSG bzw. ab dem 25.05.2018 den Voraussetzungen von Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer den Unterauftragnehmer den Subunternehmer dieselben Datenschutzpflichten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(6) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Wartungs- und Prüfungsleistungen i.S.d. § 11 Abs. 5 BDSG stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden. Die Parteien sind sich darüber einig, dass vorgenannte Wartungs- und Prüfleistungen eine „Auftragsverarbeitung“ i.S.d. Art. 28 DSGVO darstellen.

Datengeheimnis / Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG bzw. ab dem 25.05.2018 zu Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet werden. Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i.S.d. § 88 TKG zu verpflichten.

(3) An die Stelle der Wahrung des Datengeheimnisses tritt mit Wirkung vom 25.05.2018 eine Vertraulichkeitsverpflichtung des Auftragnehmers. Der Auftragnehmer wird alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, in schriftlicher Form verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln. Diese Verpflichtung der Beschäftigten ist auf Anfrage dem Auftraggeber nachzuweisen.

Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als „Anlage 2“ zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

(4) Spätestens ab dem 25.05.2018 wird der Auftragnehmer dem Auftraggeber die von ihm nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung des nach Art. 32 DSGVO und des in diesem Vertrag geregelten Schutzniveaus in dokumentierter Form und in geeigneter Weise zur Verfügung stellen. Sofern die Parteien nicht gesondert vereinbaren, dass die in der „Anlage 2“ aufgeführten technischen und organisatorischen Maßnahmen durch die nach diesem Absatz neu zur Verfügung gestellte Dokumentation der technischen und organisatorischen Maßnahmen zur Datensicherheit ersetzt werden, bleiben die in „Anlage 2“ genannten Maßnahmen Vertragsbestandteil und sind vom Auftragnehmer entsprechend zu erfüllen.

Dauer des Auftrags

(1) Der Vertrag beginnt am _____ und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.



(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer



Anlage 1

Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

E-Mail-Kommunikation:

domainfactory GmbH
Oskar-Messter-Str. 33
85737 Ismaning
Deutschland

Tel: +49 89 998 288 026
Fax: +49 89 55 266 222
E-Mail: support@df.eu

Geschäftsführer:
Dr. Claus Boyens, Tobias Mohr

Handelsregister:
Amtsgericht München, HRB 150294

Bundesnetzagentur:
BnetzA Reg-Nr. 09/330

USt.-ID-Nr:
DE813084387



Versanddienstleister:

DHL Paket GmbH
Sträßchensweg 10
53113 Bonn
Deutschland

Tel: +49 22 81 820
Fax: +49 89 55 266 222
E-Mail: impressum.paket@dhl.com

Geschäftsführer:
Norman Chmiel
Dr. Achim Dünnwald
Heinrich Eilers
Christian Metzner
Vorsitzender des Aufsichtsrates:
Uwe Brinks

Handelsregister:
Registergericht Bonn HRB 19565

USt.-ID-Nr:
DE 813312787

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers gemäß § 9 BDSG

Hinweis (kann nach vollständiger Angabe der Maßnahmen gelöscht werden): Bitte geben Sie nachfolgend jeweils die getroffenen technischen und organisatorischen Maßnahmen an. Als Unterstützung sind hier bestimmte typische Begriffe als Hilfe und Veranschaulichung angeführt.

Bei einzelnen Maßnahmen kann eine stichwortartige Benennung oder auch nur ein Wort (z.B. „Alarmanlage“) ausreichend sein. Bei anderen Maßnahmen sollte jedoch regelmäßig eine kurze Beschreibung erfolgen, die eine Bewertung durch den Auftraggeber ermöglicht (Beispiel: Im Falle einer Videoüberwachung als Maßnahme der Zutrittskontrolle wäre es erforderlich, zu beschreiben, ob z.B. nur die Eingangstür oder auch andere Gebäudeteile überwacht werden und ob eine Aufzeichnung der Aufnahmen erfolgt). Auch bei einer Maßnahme wie einer „Passwortvergabe“ ist konkret aufzuführen, ob es eine Mindestpasswortlänge und –komplexität gibt und wie Passwortlänge und Komplexität ausgestaltet sind. Außerdem wäre zudem anzugeben, ob die Mindestpasswortlänge und –komplexität technisch erzwungen wird.

Zutrittskontrolle

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

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Schließsystem mit Codesperre
- Manuelles Schließsystem
- Biometrische Zugangssperren
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen

Zugangskontrolle

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

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren

Authentifikation mit Benutzername / Passwort
Zuordnung von Benutzerprofilen zu IT-Systemen
Gehäuseverriegelungen
Einsatz von VPN-Technologie
Sperrungen von externen Schnittstellen (USB etc.)
Sicherheitsschlösser
Schlüsselregelung (Schlüsselausgabe etc.)
Personenkontrolle beim Pförtner / Empfang
Protokollierung der Besucher
Sorgfältige Auswahl von Reinigungspersonal
Sorgfältige Auswahl von Wachpersonal
Tragepflicht von Berechtigungsausweisen
Einsatz von Intrusion-Detection-Systemen
Verschlüsselung von mobilen Datenträgern
Verschlüsselung von Smartphone-Inhalten
Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
Einsatz von Anti-Viren-Software
Verschlüsselung von Datenträgern in Laptops / Notebooks
Einsatz einer Hardware-Firewall
Einsatz einer Software-Firewall

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.

Typische Maßnahmen (nur Stichworte) sind z.B.:

Erstellen eines Berechtigungskonzepts
Verwaltung der Rechte durch Systemadministrator
Anzahl der Administratoren auf das „Notwendigste“ reduziert
Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
Sichere Aufbewahrung von Datenträgern
physische Löschung von Datenträgern vor Wiederverwendung
ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
Protokollierung der Vernichtung
Verschlüsselung von Datenträgern

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 Einrichtungen zur Datenübertragung vorgesehen ist.

Typische Maßnahmen (nur Stichworte) sind z.B.:

Einrichtungen von Standleitungen bzw. VPN-Tunneln

Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

E-Mail-Verschlüsselung

Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen

Beim physischen Transport: sichere Transportbehälter/-verpackungen

Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

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.

Typische Maßnahmen (nur Stichworte) sind z.B.:

Protokollierung der Eingabe, Änderung und Löschung von Daten

Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle

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

Typische Maßnahmen (nur Stichworte) sind z.B.:

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG

Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

Auftragnehmer hat Datenschutzbeauftragten bestellt

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Vertragsstrafen bei Verstößen

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Typische Maßnahmen (nur Stichworte) sind z.B.:

Unterbrechungsfreie Stromversorgung (USV)

Klimaanlage in Serverräumen

Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

Schutzsteckdosenleisten in Serverräumen

- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze

Trennungsgebot

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

Typische Maßnahmen (nur Stichworte) sind z.B.:

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Logische Mandantentrennung (softwareseitig)

Erstellung eines Berechtigungskonzepts

Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

Versehen der Datensätze mit Zweckattributen/Datenfeldern

Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

Festlegung von Datenbankrechten

Trennung von Produktiv- und Testsystem