

AGB Auftragsdatenverarbeitung

Vereinbarung betreffend die Überlassung von Daten zum Zweck der Verarbeitung als Dienstleistung

§ 1 Gegenstand der Vereinbarung

Die nachstehenden Allgemeinen Geschäftsbedingungen für die Auftragsdatenverarbeitung (AGB-Auftragsdatenverarbeitung) gelten für alle Aufträge der Janssen-Cilag GmbH, Neuss (nachfolgend Auftraggeber oder **JC** genannt). Sie erfassen alle Aufträge mit den Vertragspartnern (nachfolgend Auftragnehmer), bei denen Daten von Menschen (§ 3 Abs. 1 Bundesdatenschutzgesetz - **BDSG**) im Auftrag verarbeitet werden (Art. 17 der EU-Richtlinie). Sie sind vorrangig gegenüber sonstigen vertraglichen Bedingungen, insbesondere des Hauptvertrags, der Leistung und Gegenleistung beschreibt. Abweichende Bedingungen darf JC aufgrund Gesetzes nicht anerkennen (§ 11 BDSG). Diese Regelungen gelten entsprechend auch für alle sonstigen im Auftrag verarbeiteten Daten.

§ 2 Parteien der Vereinbarung

Der Auftragnehmer wird personenbezogene Daten im Auftrag von JC verarbeiten. JC bleibt Inhaberin der Daten und darf allein – im Rahmen ihrer Datenschutzbefugnisse – über die Daten verfügen. Erlaubt sind nur die im Einzelauftrag angegebenen Arbeiten.

§ 3 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist gesetzlich der Auftraggeber verantwortlich (Verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG). An der Wahrung der Rechte der Betroffenen wirkt der Auftragnehmer nach Maßgabe dieser AGB-Auftragsdatenverarbeitung mit.

(2) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen. Auf den Zugang des schriftlichen (Teil-)Auftrags vom Auftraggeber wird nach § 151 BGB verzichtet; die Übersendung der Datensätze genügt.

(3) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Dies gilt entsprechend für den Auftragnehmer.

(5) Die Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von nicht öffentlich bekannten Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich zu behandeln.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer sichert zu, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den Weisungen des Auftraggebers zu verwenden und ausschließlich dem Auftraggeber zurückzugeben oder nur nach dessen schriftlichem Auftrag zu übermitteln. Die Auftragsdatenverarbeitung ist auf die in der Einzelweisung bezeichneten Daten beschränkt.

(2) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten getrennt von sonstigen Datenbeständen bearbeitet werden.

(3) Datenträger, die der Auftraggeber dem Auftragnehmer zur Verarbeitung zur Verfügung stellt, werden vom Auftragnehmer nur im Rahmen der ordnungsmäßigen Vertragsabwicklung kopiert, namentlich für Zwecke der Datensicherung. Solche Kopien werden physisch gelöscht, wenn die Kenntnis der Daten weder für die Auftragsdurchführung noch zu Beweis Zwecken mehr notwendig ist, spätestens im Zuge routinemäßiger Bestandsbereinigungen. Entsprechendes gilt für jegliche Kopien, Zwischenspeicherungen, Sicherungsbänder, Test- und Ausschussmaterial. Etwaig übergebene Originale (Originaldatenträger) sind erst nach Zustimmung des Auftraggebers zu löschen und bis

dahin zu sperren. Weicht der Auftragnehmer von dieser Anforderung ab, hat er die Kosten einer Wiederherstellung zu tragen. Der Auftraggeber ist alternativ berechtigt, den Schaden aus dem Verlust der Daten einzufordern. Soweit die Daten beim Auftraggeber noch vorhanden sind, wird im Falle vertragswidriger Löschung vermutet, dass diese Daten mit den an den Auftraggeber gelieferten Daten in Aufbau und Inhalt identisch sind.

(4) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Zuvor ist die schriftliche Zustimmung des Auftraggebers einzuholen. Absatz 3 bleibt unberührt. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

(5) Der Auftragnehmer stellt sicher, dass Makulatur mit personenbezogenen Daten entweder durch hausinterne Aktenvernichter oder von spezialisierten Entsorgungsunternehmen vernichtet werden, die die Vernichtung schriftlich garantieren und bestätigen. Die Bestätigung ist dem Auftraggeber auf Anforderung unverzüglich in Kopie auszuhändigen.

(6) Die Einschaltung von Subauftragnehmern ist ausgeschlossen, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart wird. In jedem Fall sind die Inhalte dieser AGB-Auftragsdatenverarbeitung beim Subauftragnehmer zu gewährleisten und der Auftragnehmer bleibt für die Erfüllung der auf den Subunternehmer übertragenen Tätigkeiten im gleichen Umfang verantwortlich als würden diese durch den Auftragnehmer selbst ausgeführt. Die Verpflichtungen dieser AGB sind zugleich unmittelbar gegenüber dem Auftraggeber zu begründen.

(7) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Die erforderlichen Informationen wird der Auftragnehmer dem Auftraggeber zu jeder Zeit überlassen.

(8) Der Auftragnehmer trägt für die technischen und organisatorischen Voraussetzungen Sorge, dass der Auftraggeber die Pflichten zur Auskunftserteilung sowie zur Berichtigung oder Löschung nach dem BDSG gegenüber dem Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber unverzüglich alle dafür notwendigen Informationen.

(9) Der Auftragnehmer übereignet dem Auftraggeber zur Sicherheit die Datenträger, auf denen sich Dateien befinden, die ausschließlich Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

(10) An der Erstellung der Verfahrensbeschreibung und - im Bedarfsfall - der Vorbereitung der Vorabkontrolle nach § 4d Abs. 5 Satz 1 BDSG hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

(11) 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 verständigen.

(12) Der Auftraggeber ist nach § 42a BDSG verpflichtet, ungewollte oder unrechtmäßige gesetzlich relevante Datenabflüsse an Dritte mit schwerwiegenden Beeinträchtigungen für die Betroffenen der deutschen Aufsichtsbehörde und den Betroffenen mitzuteilen. Um dieser Pflicht zu genügen, wird der Auftragnehmer den Auftraggeber über Verstöße gegen Datenschutz- oder Datensicherheitsvorschriften und gegen die in dieser Vereinbarung getroffenen Bestimmungen innerhalb von 2 Werktagen schriftlich unterrichten.

§ 5 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 5 BDSG zu wahren. Diese Pflicht ist zeitlich unbeschränkt und gilt – wie die weiteren datenschutzrechtlichen Pflichten – auch nach Beendigung des Vertrages fort.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG verpflichtet und sie mit den maßgebenden Bestimmungen und Vorgaben des Datenschutzes und der Datensicherheit hinreichend vertraut gemacht hat.

Er hat diese Verpflichtung und die Unterweisungen dokumentiert und wird die Dokumentationen der Verpflichtungen und Unterweisungen auf Anforderung dem Auftraggeber vorlegen. Insbesondere muss die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer fortgelten. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten. Der Auftragnehmer überwacht und dokumentiert die Einhaltung der datenschutzrechtlichen Vorschriften. Die Beschäftigten des Auftragnehmers dürfen nur auf einer need-to-know-Basis Zugang zu den Daten des Auftraggebers erhalten. Eine Liste der Beschäftigten, die auf die Daten Zugriff haben, ist dem Auftraggeber auf Anforderung sofort vorzulegen.

(3) Der Auftragnehmer verpflichtet sich, Änderungen der datenschutzrechtlichen Vorschriften zu beobachten und seine Mitarbeiter davon in dokumentierter Weise zu unterrichten. Die Dokumentation ist auf Anforderung des Auftraggebers vorzulegen.

(4) Auskünfte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen, sofern nicht das Gesetz etwas anderes vorsieht. Sollte der Auftragnehmer zur Herausgabe gesetzlich verpflichtet sein, so hat er die gesetzliche Weisung, die Begründung und die Ausführung dem Auftraggeber sofort schriftlich mitzuteilen.

(5) Der Auftragnehmer verpflichtet sich im Übrigen, alle ihm im Rahmen seiner Beauftragung vom Auftraggeber zur Verfügung gestellten Geschäfts- und Betriebsunterlagen und personenbezogenen Daten ordnungsgemäß aufzubewahren, so dass insbesondere Dritte keine Einsicht nehmen können. Der Auftragnehmer ist nicht berechtigt, an solchen Unterlagen ein Zurückbehaltungsrecht auszuüben. Er verpflichtet sich weiter, über den Inhalt und Gegenstand der Geschäftsverbindung mit dem Auftraggeber Stillschweigen gegenüber Dritten zu bewahren und damit keine Werbung zu betreiben. Der Auftragnehmer wird hinsichtlich der durch die Tätigkeit für den Auftraggeber erlangten Betriebs- und Geschäftsgeheimnisse, auch soweit sie sich auf Gruppengesellschaften oder Dritte beziehen, strengstens Stillschweigen bewahren. Die Verpflichtungen dieses Absatzes gelten auch nach Beendigung dieser Vereinbarung uneingeschränkt weiter.

§ 6 Datensicherheitsmaßnahmen

(1) Der Auftragnehmer garantiert, dass er ausreichende technische und organisatorische Sicherheitsmaßnahmen im Sinne des § 9 BDSG ergriffen hat. Dabei handelt es sich insbesondere um Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und gegen jede andere Form der unrechtmäßigen Verarbeitung schützen. Es sind die international anerkannten Schutzziele der Informationssicherheit, nämlich die Ziele der Verfügbarkeit, der Vertraulichkeit, der Integrität und der Prüfbarkeit, zu gewährleisten. Die Dokumentation muss auf die Gliederung der Anlage zu § 9 BDSG Rücksicht nehmen. Hinsichtlich der notwendigen Maßnahmen wird ergänzend und erläuternd auf die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwiesen, die einen möglichen Maßstab darstellen. Die technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung anzupassen und angemessen einzurichten. Wesentliche Änderungen sind schriftlich mitzuteilen. **Die Dokumentation muss auf die Gliederung der Anlage zu § 9 BDSG Rücksicht nehmen und ist dem Auftraggeber auf Anforderung jederzeit auszuhändigen** (siehe auch § 7 Abs. 2 dieser AGB Auftragsdatenverarbeitung).

(2) Der Auftragnehmer ist nicht befugt, bei der Entwicklung von Software Daten zu verwenden. Es ist mit anonymisierten Original- oder fiktiven Testdaten zu arbeiten. Die Verarbeitung der Daten in Privatwohnungen ist nur mit Einwilligung des Auftraggebers im Einzelfall gestattet.

(3) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen dieses Vertrags oder weiterer Anweisungen nicht genügen, benachrichtigt er den Auftraggeber unverzüglich schriftlich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Er unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, wenn sie

nicht geändert oder vom Auftraggeber ausdrücklich bestätigt wird.

§ 7 Überwachungsrechte des Auftraggebers

(1) Der Auftraggeber ist gesetzlich dazu verpflichtet, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen, personellen und organisatorischen Datensicherheitsmaßnahmen zu überzeugen. Hierfür wird dem Auftraggeber hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen, der gespeicherten Daten und der Datenverarbeitungsprogramme vor Ort eingeräumt. Der Auftragnehmer ist zur Duldung verpflichtet und hat erforderliche Dokumente herauszugeben und Antworten auf Fragen schriftlich in angemessener Frist zu geben. Vorliegende Prüfungsberichte mit Datenschutzbezug sind dem Auftraggeber zur Einsicht in Kopie zu überlassen. Der Auftraggeber ist zudem berechtigt, Auskünfte über den Auftragnehmer einzuholen.

(2) Der Auftragnehmer hält eine Verfahrensdokumentation bereit, die den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) hinsichtlich der Punkte Internes Kontrollsystem, Datensicherheit sowie Dokumentation und Prüfbarkeit entspricht. Wesentliche Änderungen sind dem Auftraggeber sofort schriftlich anzuzeigen. Diese Verfahrensdokumentation ist erforderlich, damit der Auftraggeber seiner gesetzlichen Pflicht zur Dokumentation seiner Datensicherheitsprüfung nachkommen kann.

(3) Der Auftraggeber kann sich ohne eigene Kontrollen über die Angemessenheit der gesetzlichen Datensicherheitsmaßnahmen überzeugen, wenn ihm der Auftragnehmer entsprechende Nachweise vorlegt, wie beispielsweise ein hinreichendes Datensicherheitskonzept, Berichte der zuständigen Datenschutz-Aufsichtsbehörde zur Datensicherheit, von der Revision, von einer anerkannten Wirtschaftsprüfungsgesellschaft oder vom betrieblichen Datenschutzbeauftragten, Nachweis einer Zertifizierung nach ISO 27001 oder Nachweis einer Auditierung nach den Regeln von branchentypischen „Verhaltensregeln“ im Sinne der EU-Datenschutzrichtlinie. Die Nachweise sollten nicht älter als zwei Jahre sein. Der Auftraggeber entscheidet nach eigenem Ermessen, ob er dergleichen Nachweise anerkennt oder nicht. Von einer aufsichtsbehördlichen Prüfung – schriftlich und/oder vor Ort – und/oder ihrer Ankündigung ist der Auftraggeber innerhalb von 3 Werktagen schriftlich in Kenntnis zu setzen.

§ 8 Vertragsdauer

Der Auftraggeber kann den Einzelvertrag/die Einzelverträge jederzeit ohne Einhaltung einer Frist kündigen, wenn eine Handlung des Auftragnehmers gegen diese AGB-Auftragsdatenverarbeitung verstößt oder es durch eine solche Handlung zu einem Verstoß des Auftragnehmers gegen die Bestimmungen des BDSG kommt, der Auftragnehmer eine datenschutzrelevante Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer die Ausübung der Überwachungsrechte des Auftraggebers nach § 7 dieser AGB-Auftragsdatenverarbeitung nicht duldet. Die weiteren Rechte des Auftraggebers bleiben unberührt. Die datenschutzbezogenen Pflichten des Auftragnehmers bleiben auch nach Kündigung dieses Vertrages wirksam, soweit gesetzlich zulässig.

Im Übrigen gelten die Regelungen des Hauptvertrags.

§ 9 Haftung

Der Auftragnehmer haftet dem Auftraggeber für datenschutzbezogene Schäden, die der Auftragnehmer, seine Mitarbeiter oder die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

§ 10 Nichterfüllung der Leistung

Der Auftragnehmer gewährleistet für einen Zeitraum von zwei Jahren ab Erbringung der Datenverarbeitungsleistungen, dass diese nicht mit Mängeln behaftet sind, die die Tauglichkeit oder den Wert der Datenverarbeitung gemäß den üblichen und vereinbarten Spezifikationen aufhebt oder nicht nur unerheblich mindert.

§ 11 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 12 Sonstiges

Die Pflichten des Auftragnehmers, die den Umgang mit den unternehmens- und/oder personenbezogenen Daten betreffen, gelten auch nach Ende des Einzelvertrages fort, bis sie nach dem zulässigen Verfahren gelöscht sind.

Soweit die Parteien per E-Mail in Verbindung treten, werden sie die Vertraulichkeit beachten, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Parteien Verschlüsselungsverfahren abstimmen.

Es gilt subsidiär die Internet-Datenschutzerklärung (Privacy Policy) des Auftraggebers, die Sie auf der Janssen-Cilag-Website <http://www.janssen-cilag.de> unter dem Link "Datenschutzerklärung" in der jeweils aktuellen Fassung abrufen können.