

Vereinbarung

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3
Datenschutz-Grundverordnung (DS-GVO)

zwischen

– Auftraggeber –

und

Wolanski GmbH
Ernst-Robert-Curtius-Str. 6
53117 Bonn

– Auftragnehmer –

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit der Zusammenarbeit in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Abrechnungsdaten, Zahlungsdaten
- Sonstiges (bitte ausfüllen): _____

Die Kategorien durch die Verarbeitung betroffener Personen umfassen:

- Kunden
- Interessenten
- Lieferanten
- Ansprechpartner
- Handelsvertreter
- Abonnenten
- Sonstiges (bitte ausfüllen): _____

Diese Vereinbarung richtet sich nach der Laufzeit der Zusammenarbeit, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
- (2) Die Weisungen werden anfänglich festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die in der Leistungsbeschreibung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisationsgestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Das Datenschutz- und Datensicherheitskonzept der Wolanski GmbH hängt dieser Vereinbarung an.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vereinbarte Schutzniveau nicht unterschritten wird.

- (3) Der Auftragnehmer unterstützt – soweit vereinbart – den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Entstehen hierdurch zusätzliche Kosten, so trägt diese der Auftraggeber.
- (4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
- (6) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- (7) Der Ansprechpartner des Auftragnehmers für im Rahmen der Vereinbarung anfallende Datenschutzfragen ist Herr Karsten Wolf (datenschutz@wolanski.de). Im Falle eines Wechsels des Ansprechpartners, unterrichtet der Auftragnehmer den Auftraggeber unverzüglich.
- (8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- (9) Der Auftragnehmer berichtigt oder löscht die auftragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren. Entstehen hierdurch zusätzliche Kosten, so trägt diese der Auftraggeber.

- (10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
- (11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Entstehen hierdurch zusätzliche Kosten, so trägt diese der Auftraggeber.

§ 4 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftrags-ergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend. Entstehen hierdurch zusätzliche Kosten, so trägt diese der Auftraggeber.
- (3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist.
- (2) Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

- (1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
- (2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
- (3) Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
- (4) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

- (1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
- (2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
- (3) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.
- (4) Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund gegenüber der vom Auftragnehmer bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.
- (5) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

- (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Zusammenarbeit vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
- (4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

WOLANSKI GMBH
Ernst-Robert-Curtius-Str. 6 53117 Bonn
Tel. 0228/55580-0 Fax 0228/55580-33
Am Stichkanal 24 14167 Berlin
Tel. 030/847982-0 Fax 030/847982-28
www.wolanski.de

Datum, Unterschrift
Auftraggeber

Datum, Unterschrift
Wolanski GmbH

Datenschutz- und Datensicherheitskonzept

entsprechend Art. 5 Abs. 1 lit. f und Art. 32 DSGVO

Dem Schutz der personenbezogenen Daten der betroffenen Personen kommt höchste Bedeutung zu. Die personenbezogenen Daten sind daher stets in Übereinstimmung mit den anwendbaren Datenschutzvorschriften, insbesondere der Datenschutzgrundverordnung (DSGVO) zu verarbeiten.

Gem. Art. 32 DSGVO sind die zu treffenden technischen und organisatorischen Maßnahmen im Einzelnen festzulegen. Dies erfolgt innerhalb dieses Datenschutz- und Datensicherheitskonzepts.

Entsprechend Art.32 DSGVO hat die Wolanski GmbH die technischen und organisatorischen Maßnahmen zu treffen, die geeignet sind, um die Ausführung der Vorschriften der DSGVO zu gewährleisten. Geeignet sind Maßnahmen nur, wenn sie eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung. Dazu wurde eine vorangehende Bewertung von Risiko und Folgen für die Rechte und Freiheiten betroffener Personen unter Berücksichtigung der Art der Auftragsdaten, des Umfangs, der Umstände, des Zwecks, der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos, des Stands der Technik, der Implementierungskosten sowie der notwendigen Garantien zum Schutz der betroffenen Personen durchgeführt.

Allgemeine Datenschutzgrundsätze

Die Wolanski GmbH setzt bei der Verarbeitung personenbezogener Daten nur Personal ein, welches geschult und zur Einhaltung der datenschutzrechtlichen Vorgaben und Verhaltensregeln verpflichtet ist. Dies trifft ebenso die Mitarbeiter des Auftragsverarbeiters. Die letzte unternehmensweite Schulung fand im September 2017 statt. Nach diesem Termin neu eingetretenes Personal wurde jeweils gesondert eingewiesen und zur Vertraulichkeit verpflichtet.

Das Unternehmens-LAN ist durch eine Firewall nach dem aktuellsten Stand der Technik gegen Angriffe aus dem Internet geschützt. Bei der Identifizierung und Umsetzung von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik hält sich die Wolanski GmbH an den IT-Grundschutz.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Zutrittskontrolle

Die Wolanski GmbH verwehrt Unbefugten den Zutritt zu den Unternehmensräumen. Dies geschieht durch:

- Einsatz eines Objektschutzes (inkl. nächtlicher Rundgänge)
- Einsatz eines Schließsystems, das einen Zugang nur für Berechtigte ermöglicht
- Permanente Begleitung bzw. Beaufsichtigung von Besuchern
- Baulich separierter Serverraum inkl. Verwendung eines Chip-Kartenzugangssystems für den Bereich IT

• Zugangskontrolle

Die Wolanski GmbH verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies geschieht durch:

- Authentifizierung von Systemanwendern durch Benutzer-/Passwortverfahren
- Einrichtung persönlicher Benutzerkonten zur Steuerung individueller Berechtigungen
- Protokollierung von Einwahlversuchen
- Sperrung von Benutzerkonten nach drei Fehlversuchen
- Passwörter müssen folgende Restriktionen erfüllen: Länge mind. acht Zeichen, Gültigkeit 6 Monate, Passwort-Historie über die letzten 5 Einträge
- Automatische Bildschirmsperrung nach 5 Minuten Inaktivität
- Unverzügliche Sperrung des Benutzers bei Austritt (Verwendung eines Laufzettels)

- **Zugriffskontrolle**

Die Wolanski GmbH gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Datenverschlüsselung auf der gesamten Datenverbindungsstrecke, also zwischen Kunde und der Wolanski GmbH.
- Erstellung von Übermittlungsprotokollen
- Berechtigungsvergaben erfolgen durch Anmeldeprofile für die verschiedenen Funktionsbereiche. Es findet eine einmalige Festlegung der Berechtigungen statt. Bei Nutzerwechseln erfolgt eine Sperrung des nicht mehr verwendeten Accounts. Der neue Nutzer wird durch das Einsetzen in seinen Funktionsbereich automatisch mit den notwendigen Berechtigungen ausgestattet. Die Zugriffsrechte sind ausreichend differenziert und erfüllen das Need-to-know-Prinzip.
- Papierunterlagen werden über geeignete Entsorgungscontainer gesammelt und einem zuverlässigen Entsorgungsunternehmen zur Vernichtung übergeben.

- **Trennungskontrolle**

Die Wolanski GmbH gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies geschieht durch:

- Mandantentrennung durch logische Datentrennung auf Basis von Kunden- und Mandantennummern
- Vergabe von Zugriffsrechten

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Eingabekontrolle**

Die Wolanski GmbH gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Organisatorische Festlegung von Zuständigkeiten
- Zugriffssteuerung / Erfassungsprotokolle
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines geeigneten Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

Die Wolanski GmbH gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

- Regelmäßige Anfertigung von Datensicherungen (tägliche Erstellung von Sicherheitskopien)
- Auslagerung der Backupmedien an einen brandgeschützten Lagerungsort
- Einsatz einer unterbrechungsfreien Stromversorgung für Server
- Klimatisierte Serverräume mit Brandmeldern

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Wolanski GmbH gewährleistet, dass die Wirksamkeit der technisch organisatorischen Maßnahmen (TOM) regelmäßig durch geeignete Verfahren einer kritischen Begutachtung unterzogen und die daraus resultierenden Ergebnisse in regelmäßigen Abständen bewertet sowie die notwendigen Anpassungsmaßnahmen vorgenommen werden. Dies geschieht durch:

- **Incident-Response-Management**

- Firewalls regelmäßig auf Updates hin überprüfen und diese auf die Systeme laden
- USV regelmäßig kontrollieren
- Überprüfung der Wiederherstellbarkeit von Backup-Dateien

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

- **Auftragskontrolle**

Die Wolanski GmbH gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dies geschieht durch:

- Abstimmung in der Auftragsorganisation mit dem Auftraggeber
- Auftragsbezogene Protokollierungen und Kontrollmechanismen (Vollständigkeit, Durchlauf der Produktionskette)
- Schulung und Information der Mitarbeiter

Ansprechpartner

Für alle Fragen rund um den Datenschutz bei der Wolanski GmbH steht Ihnen der betriebliche Datenschutzbeauftragte zur Verfügung:

Karsten Wolf
Wolanski GmbH
Ernst-Robert-Curtius-Str. 6
53117 Bonn-Buschdorf

Tel.: 0228/55580-512
E-Mail: datenschutz@wolanski.de