

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) - ToolScan

Auftraggeber	Der jeweilige Vertragspartner der Bavaria Systems GmbH aus dem Hauptvertrag über die Nutzung von ToolScan (nachfolgend „Auftraggeber“). Eine gesonderte Eintragung von Firma, Anschrift oder Vertretungsberechtigten in dieser Vereinbarung ist nicht erforderlich.
Auftragnehmer	Bavaria Systems GmbH, Osterhofener Str. 16, 93055 Regensburg, vertreten durch den Geschäftsführer Florian Buchfink (nachfolgend „Auftragnehmer“).

Diese Vereinbarung ergänzt den zwischen den Parteien bestehenden Hauptvertrag über ToolScan. Sie gilt für alle Verarbeitungsvorgänge, bei denen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Die Zuordnung des Auftraggebers erfolgt ausschließlich über den jeweiligen Hauptvertrag bzw. das zugehörige Kundenkonto.

1. Gegenstand und Dauer der Verarbeitung

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers, soweit dies zur Bereitstellung, zum Betrieb, zur Wartung, zum Support und zur vertragsgemäßen Nutzung von ToolScan erforderlich ist.

1.2 Die Verarbeitung erfolgt für die Dauer des Hauptvertrags. Soweit technisch oder rechtlich erforderlich, schließt sich eine angemessene Abwicklungs-, Export- und Löschphase an. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

1.3 Die Verarbeitung erfolgt ausschließlich im Rahmen dieser Vereinbarung, des Hauptvertrags und dokumentierter Weisungen des Auftraggebers, soweit keine gesetzliche Verpflichtung zu einer abweichenden Verarbeitung besteht.

2. Art, Zweck und Umfang der Verarbeitung

2.1 Zweck der Verarbeitung ist die Bereitstellung einer Softwarelösung zur digitalen Verwaltung von Werkzeugen, Geräten, Lagerplätzen, Ausgaben, Rücknahmen, Reservierungen, Wartungen, Reparaturen und vergleichbaren betrieblichen Vorgängen einschließlich Nutzerverwaltung, technischer Administration und Support.

2.2 Die Verarbeitung kann insbesondere das Erheben, Erfassen, Ordnen, Speichern, Auslesen, Abfragen, Verwenden, systeminterne Übermitteln, Einschränken, Exportieren und Löschen personenbezogener Daten umfassen.

2.3 Art und Umfang richten sich nach der konkreten Nutzung von ToolScan durch den Auftraggeber. Der Auftragnehmer bestimmt grundsätzlich nicht, welche personenbezogenen Inhalte der Auftraggeber in das System einstellt.

3. Kategorien betroffener Personen und Daten

3.1 Betroffene Personen sind insbesondere Beschäftigte, Mitarbeiter und sonstige vom Auftraggeber autorisierte Nutzer von ToolScan sowie gegebenenfalls weitere Personen, deren Daten der Auftraggeber bestimmungsgemäß in ToolScan erfasst.

3.2 Verarbeitet werden können insbesondere Name bzw. Mitarbeiterbezeichnung, dienstliche Telefonnummer oder sonstige dienstliche Kontaktdaten, Benutzer- oder Mitarbeiterkennung sowie nutzungs- und vorgangsbezogene Zuordnungsdaten, insbesondere im Zusammenhang mit Ausgabe, Rücknahme, Reservierung, Wartung oder Reparatur von Werkzeugen und Geräten.

3.3 Soweit der Auftraggeber zusätzliche Inhalte wie Notizen, Fotos, Dokumente oder Anhänge einstellt, können auch darin enthaltene personenbezogene Daten verarbeitet werden. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind für die gewöhnliche Nutzung von ToolScan nicht vorgesehen.

4. Weisungsgebundene Verarbeitung

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Weisungen ergeben sich zunächst aus dem Hauptvertrag, dieser Vereinbarung und der bestimmungsgemäßen Nutzung der Software. Zusätzliche Weisungen können in Textform erteilt werden.

4.2 Ist der Auftragnehmer aufgrund von Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, informiert er den Auftraggeber vor der Verarbeitung über diese rechtliche Anforderung, soweit eine solche Mitteilung gesetzlich zulässig ist.

4.3 Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, weist er den Auftraggeber darauf hin und kann die Ausführung bis zur Klärung aussetzen.

5. Vertraulichkeit und Personal

5.1 Der Auftragnehmer stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.2 Zugriffe auf personenbezogene Kundendaten werden auf Personen beschränkt, die diese für ihre Aufgaben benötigen. Berechtigungen werden nach dem Erforderlichkeitsprinzip vergeben und bei Wegfall des Bedarfs entzogen.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

6.2 Die wesentlichen Maßnahmen sind in Anlage 1 beschrieben. Der Auftragnehmer darf einzelne Maßnahmen an technische oder organisatorische Entwicklungen anpassen, sofern das Schutzniveau insgesamt nicht wesentlich abgesenkt wird.

7. Unterstützung des Auftraggebers

7.1 Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang bei der Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO sowie bei der Bearbeitung von Betroffenenrechten, soweit dies unter Berücksichtigung der Art der Verarbeitung möglich und erforderlich ist.

7.2 Gehen Ersuchen betroffener Personen unmittelbar beim Auftragnehmer ein und sind sie erkennbar dem Auftraggeber zuzuordnen, leitet der Auftragnehmer diese grundsätzlich an den Auftraggeber weiter, sofern keine gesetzliche Verpflichtung zu einer unmittelbaren Bearbeitung besteht.

8. Datenschutzverletzungen

8.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit Daten des Auftraggebers betroffen sind.

8.2 Der Auftragnehmer stellt die ihm verfügbaren Informationen bereit, die der Auftraggeber für seine Bewertung und etwaige Meldungen nach Art. 33 und 34 DSGVO benötigt. Fehlende Informationen können nachgereicht werden.

9. Unterauftragnehmer

9.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Der Auftragnehmer verpflichtet eingesetzte Unterauftragnehmer vertraglich zu Datenschutzpflichten, die den Anforderungen des Art. 28 DSGVO entsprechen.

9.2 Der Auftragnehmer führt eine aktuelle Liste der für die Verarbeitung von ToolScan-Kundendaten eingesetzten Unterauftragnehmer und stellt diese dem Auftraggeber auf Anfrage zur Verfügung. Beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragnehmern werden dem Auftraggeber in geeigneter Weise mitgeteilt, insbesondere an eine im Hauptvertrag bzw. Kundenkonto hinterlegte Kontaktadresse.

9.3 Der Auftraggeber kann aus berechtigten datenschutzrechtlichen Gründen gegen eine beabsichtigte Änderung Widerspruch erheben. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der datenschutzrechtlichen Pflichten der von ihm eingesetzten Unterauftragnehmer verantwortlich.

10. Verarbeitung außerhalb EU/EWR

10.1 Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Soweit erforderlich, werden geeignete Garantien und ergänzende Schutzmaßnahmen eingesetzt.

11. Nachweise und Kontrollen

11.1 Der Auftragnehmer stellt dem Auftraggeber die zur Darlegung der Einhaltung von Art. 28 DSGVO erforderlichen Informationen in angemessenem Umfang zur Verfügung und ermöglicht erforderliche Kontrollen.

11.2 Vorrangig sollen schriftliche Auskünfte, vorhandene Dokumentationen, Prüfberichte oder vergleichbare Nachweise genutzt werden. Vor-Ort-Prüfungen sind mit angemessener Frist anzukündigen und so durchzuführen, dass Betriebsabläufe sowie Vertraulichkeits- und Sicherheitsinteressen anderer Kunden nicht unangemessen beeinträchtigt werden.

12. Datensicherung, Wiederherstellung und Verfügbarkeit

12.1 Kundendaten werden im Rahmen eines internen Sicherungs- und Wiederherstellungskonzepts regelmäßig gesichert. Sicherungskopien werden technisch und organisatorisch gegen unbefugten Zugriff geschützt.

12.2 Sicherungen dienen der Wiederherstellung nach technischen Störungen, Datenverlust oder vergleichbaren Ereignissen und werden nicht als paralleles Produktivsystem genutzt. Sicherungs- und Wiederherstellungsverfahren werden risikoorientiert überprüft und an technische Änderungen angepasst.

12.3 Sicherungskopien unterliegen definierten Aufbewahrungs-, Überschreibungs- und Löschzyklen. Eine dauerhafte oder zeitlich unbegrenzte Speicherung in Sicherungssystemen ist nicht geschuldet.

13. Datenexport und Löschung bei Vertragsende

13.1 Nach Abschluss der vertraglich vereinbarten Verarbeitung stellt der Auftragnehmer auf Weisung des Auftraggebers einen technisch angemessenen Export der exportierbaren Kundendaten bereit oder löscht die personenbezogenen Daten, soweit keine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

13.2 Ein gewünschter Abschluss-Export soll rechtzeitig vor Vertragsende angefordert werden. Die Bereitstellung erfolgt in einem gängigen, technisch verfügbaren und maschinenlesbaren Format, soweit dies für die jeweilige Datenart möglich ist. Dateien und Anhänge können, soweit technisch vorgesehen, in ihrem gespeicherten oder einem geeigneten gebräuchlichen Format bereitgestellt werden.

13.3 Eine vollständige technische Migration in ein System eines Drittanbieters oder die Herstellung eines bestimmten Fremdformats ist nur geschuldet, wenn dies gesondert vereinbart wurde.

13.4 Nach erfolgter Rückgabe bzw. nach Ablauf einer angemessenen Abwicklungsphase werden produktiv gespeicherte personenbezogene Kundendaten gelöscht oder anonymisiert, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Daten in Sicherungskopien werden im Rahmen der regulären Sicherungs- und Überschreibungszyklen entfernt und bis dahin nicht für produktive Zwecke verwendet.

14. Pflichten des Auftraggebers

14.1 Der Auftraggeber bleibt Verantwortlicher im Sinne der DSGVO. Er ist insbesondere für die Rechtmäßigkeit der Datenerhebung, die Zulässigkeit der Verarbeitung, die Erteilung rechtmäßiger Weisungen und die Wahrung der Rechte betroffener Personen verantwortlich.

14.2 Der Auftraggeber sorgt für eine angemessene Berechtigungsverwaltung seiner Nutzer und stellt sicher, dass nur solche personenbezogenen Daten in ToolScan verarbeitet werden, deren Verarbeitung für den jeweiligen Zweck zulässig ist.

15. Schlussbestimmungen

15.1 Diese Vereinbarung ist Bestandteil des zwischen Auftraggeber und Bavaria Systems GmbH bestehenden Vertragsverhältnisses. Sie wird in elektronischer Form geschlossen und bedarf keiner eigenhändigen Unterschrift.

15.2 Änderungen und Ergänzungen sollen in Textform dokumentiert werden. Zwingende gesetzliche Regelungen bleiben unberührt.

15.3 Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Soweit der Hauptvertrag wirksame Regelungen zu anwendbarem Recht und Gerichtsstand enthält, gelten diese auch für diese Vereinbarung, soweit datenschutzrechtlich zulässig.

ANLAGE 1 - TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Die nachfolgenden Maßnahmen beschreiben das allgemeine Schutzniveau für die Verarbeitung von ToolScan-Kundendaten. Konkrete Implementierungsdetails können aus Sicherheitsgründen vertraulich behandelt werden, soweit dem Auftraggeber dennoch ein angemessener Nachweis ermöglicht wird.

Bereich	Maßnahmen
1. Organisation und Vertraulichkeit	Verpflichtung berechtigter Personen auf Vertraulichkeit; datenschutzbezogene Sensibilisierung; definierte Zuständigkeiten; Zugriff nur nach Erforderlichkeit.
2. Zutritts- und physischer Schutz	Angemessene Sicherung von Betriebsräumen und Arbeitsmitteln; Auswahl externer Rechenzentrums- bzw. Cloud-Infrastruktur mit angemessenem physischem Sicherheitsniveau.
3. Zugang und Authentifizierung	Individuelle Benutzerkonten; angemessene Authentifizierungsverfahren; geregelte Vergabe, Änderung und Entziehung von Zugängen; Deaktivierung nicht mehr benötigter Konten.
4. Zugriff und Mandantentrennung	Rollen- bzw. aufgabenbezogene Berechtigungen; logische Trennung von Kundendaten; Beschränkung administrativer Zugriffe auf den erforderlichen Personenkreis.
5. Übertragungs- und Kommunikationssicherheit	Zeitgemäße Absicherung von Datenübertragungen über öffentliche Netze, soweit technisch anwendbar; geschützter Umgang mit Zugangsdaten; Begrenzung von Export- und Supportübermittlungen auf den erforderlichen Umfang.
6. Verfügbarkeit und Datensicherung	Regelmäßige Sicherungen nach internem Sicherungs- und Wiederherstellungskonzept; Schutz der Sicherungskopien vor unbefugtem Zugriff; angemessene Wiederherstellungsmaßnahmen; definierte Löscho- bzw. Überschreibungszyklen.
7. Integrität und Änderungen	Kontrollierte Umsetzung von Änderungen; risikoorientierte Behandlung sicherheitsrelevanter Aktualisierungen; möglichst keine unnötige Verwendung produktiver personenbezogener Daten in Test- und Entwicklungsumgebungen.
8. Sicherheitsvorfälle	Interne Abläufe zur Erkennung, Bewertung, Eindämmung und Dokumentation von Sicherheitsvorfällen; Kommunikation datenschutzrelevanter Vorfälle nach Maßgabe dieser AVV.
9. Überprüfung	Regelmäßige und anlassbezogene Überprüfung des Schutzniveaus; Anpassung an technische, organisatorische und rechtliche Entwicklungen.

ANLAGE 2 - INFORMATIONEN ZU DATENSICHERUNG UND DATENEXPORT**A. Datensicherung**

ToolScan-Kundendaten werden regelmäßig nach einem internen Sicherungs- und Wiederherstellungskonzept gesichert. Sicherungskopien werden gegen unbefugten Zugriff geschützt. Die Verfahren werden risikoorientiert überprüft und an technische Entwicklungen angepasst. Sicherungen dienen der Wiederherstellung und nicht dem parallelen Produktivbetrieb.

B. Datenexport

Der Auftraggeber kann einen Export seiner technisch exportierbaren Kundendaten anfordern. Ein vollständiger Abschluss-Export soll rechtzeitig vor Vertragsende abgestimmt werden. Die Bereitstellung erfolgt in einem gängigen, maschinenlesbaren Format, soweit dies für die jeweilige Datenart technisch verfügbar ist. Eine Migration in ein bestimmtes Fremdsystem ist nicht Bestandteil der gewöhnlichen Datenrückgabe.

C. Löschung

Nach Rückgabe bzw. Export und Ablauf einer angemessenen Abwicklungsphase werden produktive personenbezogene Kundendaten gelöscht oder anonymisiert, soweit keine gesetzlichen Aufbewahrungspflichten bestehen. Daten in Sicherungskopien werden mit den regulären Sicherungs- und Überschreibungszyklen entfernt.

D. Datenschutzkontakt

Anfragen zur Auftragsverarbeitung, zu Unterauftragnehmern, Datenexporten oder Löschung können an Bavaria Systems GmbH, Osterhofener Str. 16, 93055 Regensburg, E-Mail: info@bavariasystems.de gerichtet werden.

ANLAGE 3 - KURZBESCHREIBUNG DER VERARBEITUNG

Leistung	Bereitstellung und Betrieb der SaaS-Lösung ToolScan einschließlich Administration, Wartung, Support und vertragsgemäßer Systemfunktionen.
Zweck	Digitale Werkzeug- und Geräteverwaltung, Zuordnung und Nachverfolgung, Lagerorganisation, Ausgabe/Rücknahme, Reservierung, Wartungs- und Reparaturprozesse sowie Nutzerverwaltung.
Betroffene Personen	Beschäftigte, Mitarbeiter und sonstige Nutzer des Auftraggebers; gegebenenfalls weitere vom Auftraggeber erfasste Personen.
Datenarten	Insbesondere Name/Mitarbeiterbezeichnung, dienstliche Telefonnummer bzw. dienstliche Kontaktdaten, Benutzer-/Mitarbeiterkennung sowie nutzungs- und vorgangsbezogene Zuordnungsdaten; gegebenenfalls vom Auftraggeber eingestellte Notizen, Fotos, Dokumente und Anhänge.
Dauer	Dauer des Hauptvertrags zuzüglich technisch oder rechtlich erforderlicher Abwicklungs-, Export-, Löscho- und Aufbewahrungsphasen.