Richtlinie für Lieferanten

Richtlinie

Version und Datum	**V1.0**
Freigabedatum	**06.11.2025**
Verantwortlicher der Dokumentation	**Marvin Schmidt (ISB)**
Vertraulichkeitsstufe	**Öffentlich**

Freigabe des Dokumentes

Datum	Freigabe durch	Unterschrift
06.11.2025	Michaela Schuster	

Änderungshistorie

Version	Historie	Datum	Ersteller	Freigabe
V1	Erstellung	12.02.2024	Tobias Riede	GF
V1.1	Überarbeitung	06.11.2025	Marvin Schmidt	GF

Dokumentenverteiler

Berechtigte Rolle (Verteilerkreis)

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

TEAM23

Inhaltsverzeichnis

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Festlegung der verbindlichen Anforderungen und Verfahren für den Umgang mit Lieferanten und Partnern im Hinblick auf Informationssicherheit, Datenschutz und Qualitätsmanagement.
Es stellt sicher, dass externe Parteien, die Produkte, Dienstleistungen oder IT-Leistungen für Team23 erbringen, den Schutzbedarf sensibler Informationen, personenbezogener Daten sowie die Qualitätsstandards des Unternehmens einhalten.

Dieses Dokument gilt für alle Lieferanten und Partner, deren Tätigkeiten die Vertraulichkeit, Integrität, Verfügbarkeit oder Qualität von Informationen, Prozessen, Produkten oder Dienstleistungen von Team23 beeinflussen können.

Anwender dieses Dokuments sind das Top-Management, der Informationssicherheitsbeauftragte (ISB), der Datenschutzbeauftragte (DSB), die Qualitätsmanagementbeauftragten (QMB) sowie alle Mitarbeitenden von Team23, die in Auswahl, Bewertung, Beauftragung oder Überwachung von Lieferanten und Partnern eingebunden sind.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Control 6- 8 – A.8.26 / A.5.19
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Informationssicherheitspolitik
- QM-Politik
- Datenschutz-Grundverordnung (DSGVO)

3. Betroffene Lieferanten

3.1 Lieferanten und Geschäftsbeziehungen

Bewertungspflicht von Lieferanten

Unter folgenden Bedingungen müssen Lieferanten in Bezug auf Informationssicherheit, Datenschutz und Qualitätsmanagement bewertet werden.
Soweit erforderlich, sind entsprechende Zusatzvereinbarungen (z. B. zur Informationssicherheit, Auftragsverarbeitung, Qualitätssicherung) abzuschließen.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

Eine Bewertung ist erforderlich, wenn:

- ein Zugriff oder eine Verarbeitung interner oder vertraulicher Dokumente und Informationen erfolgt,
- ein Zugriff auf das interne Netzwerk, Systeme oder Cloud-Dienste von Team23 besteht,
- ein dauerhafter oder regelmäßiger Zutritt zu Geschäftsräumen gewährt wird,
- Zutrittsberechtigung zu Räumen besteht, in denen sensible oder personenbezogene Informationen verarbeitet werden,
- Wartung, Bereitstellung, Entwicklung oder Hosting sensibler IT-Systeme oder -Dienste durchgeführt wird,
- personenbezogene Daten im Auftrag von Team23 verarbeitet werden (Art. 28 DSGVO),
- oder die Risikoanalyse ergibt, dass die Lieferantenbeziehung Einfluss auf die Erreichung der Informationssicherheits-, Datenschutz- oder Qualitätsziele von Team23 haben kann.

Folgende Ausnahmen bestehen:

- Erfüllt der Vertrag oder die Leistungsbeschreibung nachweislich bereits die erforderlichen Sicherheits-, Datenschutz- und Qualitätsanforderungen (Bewertung durch ISB, DSB und ggf. QMB), kann auf eine separate Zusatzvereinbarung verzichtet werden.
- Standardisierte Lieferantenbeziehungen mit geringem Risiko (z. B. Büromaterial, Standardsoftware ohne Datenzugriff) sind von der erweiterten Bewertung ausgenommen, sofern sie im Rahmen der jährlichen Risikobewertung entsprechend eingestuft sind.

3.2 IT-Systeme

Die Beschaffung von Standardkomponenten kann ohne separate Lieferantenfreigabe erfolgen. Folgende Mindestanforderung sind hierbei zu beachten:

Kategorien	***Anforderungen***
Serverhardware	- Unterstützung von UEFI und Secure Boot - Netzteilredundanz - Supportvereinbarung (mindestens 3 Jahre vor Ort)
Clienthardware	- Secure Boot

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

4. Beauftragung von Lieferanten

Die Beauftragung eines Lieferanten, der unter die in dieser Richtlinie definierten Kriterien für betroffene Geschäftspartner fällt, darf **grundsätzlich erst nach Freigabe** durch den **Informationssicherheitsbeauftragten (ISB)**, den **Datenschutzbeauftragten (DSB)** und – sofern qualitätsrelevante Leistungen betroffen sind – den **Qualitätsmanagementbeauftragten (QMB)** erfolgen.

Vor einer Beauftragung ist sicherzustellen, dass alle relevanten Anforderungen in den Bereichen **Informationssicherheit**, **Datenschutz** und **Qualität** vertraglich geregelt sind. Hierzu gehören insbesondere:

- eine **Geheimhaltungsvereinbarung (NDA)**,
- eine **Zusatzvereinbarung mit Lieferanten** (Informationssicherheit und QM),
- sowie – bei Verarbeitung personenbezogener Daten – ein **Vertrag zur Auftragsverarbeitung (AVV)** gemäß Art. 28 DSGVO.

Die Lieferanten werden im **Informationssicherheits- und Qualitätsmanagementsystem (ISMS/QMS)** von Team23 bewertet, um die jeweilige Kritikalität und die anzuwendenden Schutzmaßnahmen festzulegen.

Für die Freigabe ist eine Risikobewertung durchzuführen, welche die Risiken der Nutzung des Lieferanten nach den folgenden Kategorien einstuft:

- **Normal:**
  Die Sicherheits-, Datenschutz- und Qualitätsmaßnahmen des Lieferanten sind dem Schutzbedarf der verarbeiteten Informationen, personenbezogenen Daten oder bereitgestellten Leistungen angemessen.
- **Hoch:**
  Die Maßnahmen des Lieferanten sind grundsätzlich angemessen, es bestehen jedoch Lücken (z. B. kein zertifiziertes ISMS/QMS, unvollständige Sicherheits- oder Datenschutznachweise, unvollständige Vertragsregelungen).
- **Sehr hoch:**
  Es ist nicht erkennbar, dass die Sicherheits-, Datenschutz- oder Qualitätsmaßnahmen des Lieferanten angemessen für das angestrebte Schutzniveau sind. Eine Zusammenarbeit ist erst nach Umsetzung risikomindernder Maßnahmen möglich.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

TEAM23 akzeptiert grundsätzlich nur Lieferanten mit einer **Risikoeinstufung bis maximal „Hoch“**.
Liegt das Risiko darüber, sind geeignete Maßnahmen (z. B. Vertragsnachbesserungen, Zusatzvereinbarungen, Lieferantenaudit, Zertifikatsnachweise) umzusetzen, bevor eine Freigabe erfolgen kann.

Unser Unternehmen akzeptiert maximal die Risikoeinstufung „Hoch“.

Liegt das Risiko mit dem Lieferanten über diesem Niveau, müssen risikomindernde Maßnahmen implementiert werden und auf Basis dessen eine neue Bewertung durchgeführt werden. Hierzu gehören:

- Nachbesserung des Vertrags
- Bestimmung von Zusatzvereinbarung oder Vertragsstrafen
- Durchführung von Lieferantenaudits, um kritische Bereiche und die Einhaltung getroffener Regeln zu prüfen
- Bereitstellung von Zertifikaten zum Nachweis

Die abzuschließenden Zusatzvereinbarungen müssen wenigstens den Mindestanforderungen aus diesem Dokument entsprechen.

Alternativ kann der vom Lieferanten bereitgestellte Vertrag durch den ISB, DSB, QMB auf diese Anforderungen geprüft werden.

Die Freigabe des Lieferanten wird durch den ISB dokumentiert und kommuniziert.

5. Überprüfung von Lieferanten

Die Risikobewertung aller Lieferanten wird mindestens einmal im Jahr überarbeitet und wiederholt.

Wird als risikominimierende Maßnahme ein Lieferantenaudit definiert, ist dies ebenfalls mindestens jährlich im Rahmen des regulären Auditprogramms einzuplanen und durchzuführen.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX

6. Mindestanforderungen an Verträge

Die Dokumentvorlage "Zusatzvereinbarung mit Lieferanten" stellt einen umfassenden und weitgehend passenden Vertrag dar sollte es keine Vereinbarung geben.

7. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab 06.11.2025.

Der Eigentümer des Dokuments ist der ISB die das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

TEAM23 GmbH, Beim Glaspalast 1, 86153 Augsburg | Tel.: 0821 / 207 085 0, Fax.: 0821 / 207 085 29,
www.team23.de | **Geschäftsführer** Fabian Ziegler, Michaela Schuster | **Registergericht Augsburg,** USt-IdNr.:DE308873371,
Registernummer: HRB 26700 | **Stadtsparkasse Augsburg,** IBAN: DE12 7205 0000 0250 6727 06, BIC: AUGSDE77XXX