BESCHAFFER-GUIDE

Zwölf Fragen an einen Softwarelieferanten für sicherheitskritische Systeme.

Ein Prüfleitfaden für Beschaffer, Programm-Manager und Fachverantwortliche in Aerospace, Defence, Automotive und kritischen Infrastrukturen.

AUSGABE	UMFANG	BAUSTEIN	ABSENDER
1 / 2026	12 Prüfpunkte	01 von 06	new direction GmbH

Softwareprojekte in sicherheitskritischen Umgebungen folgen einer anderen Logik als die tägliche Business-IT. Ein Fehler im Code lässt sich nicht durch einen unbemerkten Hotfix am nächsten Tag beheben. Er berührt Verfügbarkeit im Einsatz, Verantwortung im Betrieb und, bei staatlichen Fachanwendungen, den Bestand einer Verwaltungsleistung.

Die folgenden zwölf Fragen unterstützen Sie dabei, in einem Erstgespräch oder in einer Angebotsprüfung schnell zu erkennen, ob ein Lieferant tatsächlich beschafferfähig ist. Zwei der Fragen (elf und zwölf) betreffen Aspekte, die in Standard-Prüfkatalogen selten vorkommen, sich in der Praxis aber als hochrelevant erwiesen haben.

Jede Frage folgt derselben Struktur. Eine Kernaussage, ein Prüfhinweis, ein Kontext, ein Antwortmuster mit Substanz, ein Warnzeichen, und eine kurze Angabe zur eigenen Position von new direction. Sie können den Guide unverändert nutzen, an interne Prüfprozesse anpassen oder als Grundlage für eine schriftliche Lieferantenbefragung einsetzen.

01 Zertifizierungen im gelebten Alltag

PRÜFT: OB ZERTIFIKATE IM ENTWICKLUNGSALLTAG TATSÄCHLICH ANGEWENDET WERDEN.

Welche Zertifizierungen liegen vor, wann wurde zuletzt auditiert, und wie werden die zugehörigen Prozesse in Ihrem Entwicklungsalltag angewendet? Eine ISO 9001 reicht im sicherheitskritischen Umfeld selten aus. Relevant ist der Nachweis, dass Prozesse standardisiert und geprüft sind und dass Entwickler die Vorgaben selbst erklären können.

> ANTWORT MIT SUBSTANZ
>
> Aktuelle TISAX-Auditierung mit hohem Schutzbedarf, EcoVadis Gold oder vergleichbare Bewertung, konkrete Prüfdaten mit Ablaufhorizont, sichtbare Umsetzung in CI/CD-Pipelines und Freigabepfaden.

> WARNZEICHEN
>
> Zertifikate erscheinen dauerhaft "in Planung", Auditdaten fehlen, Entwickler kennen die zugrundeliegenden Anforderungen nicht.

NEW DIRECTION DAZU: TISAX-Auditierung 2025 bestanden, gültig bis 2028. EcoVadis Gold aktuell. ISO 27001 in Vorbereitung. Alle Entwickler durchlaufen ein achtstündiges Sicherheits- und Prozess-Onboarding.

02 Sicherheitsstatus von Standort und Personal

PRÜFT: DIE RÄUMLICHE UND PERSONELLE ZUGANGSBARRIERE ZU KLASSIFIZIERTEN INFORMATIONEN.

Ist Ihr Standort sicherheitsüberprüft, und wie viele Mitarbeitende sind zum aktuellen Zeitpunkt sicherheitsüberprüft? Für Aufträge im Verteidigungs-, Behörden- und Dual-Use-Kontext ist die räumliche und personelle Zugangsbarriere Voraussetzung, nicht Zusatz.

> ANTWORT MIT SUBSTANZ
>
> Sicherheitsüberprüfter Standort im Inland, Personal mit definiertem Prüfstatus, Onshore-Entwicklung, klare Aussage zur Zahl geprüfter Personen mit Datum.

> WARNZEICHEN
>
> Ausweichende Antworten zu Subunternehmern, verteilte Entwicklung in unklaren Rechtsräumen, Zahlen ohne Zeitbezug.

NEW DIRECTION DAZU: Sicherheitsüberprüfter Standort in Augsburg. Anteil sicherheitsüberprüften Personals im Rahmen laufender Mandate, Ausweitung in Vorbereitung. Reine Onshore-Entwicklung ohne Offshore-Anteile.

03 Standards und Normen der eigenen Domäne

PRÜFT: OB DER ANBIETER DEN EIGENEN STATUS PRO STANDARD EHRLICH BENENNEN KANN.

Nach welchen domänenspezifischen Standards arbeiten Sie (etwa DO-178C, EMAR, STANAG 4586, ISO 26262, Automotive SPICE), und wie ehrlich benennen Sie den eigenen Status pro Standard? Zulassung und Beschaffungsfähigkeit hängen weniger davon ab, dass ein Anbieter Standards kennt, als davon, dass er die Nachweise (Traceability, Testabdeckung, Dokumentation) tatsächlich liefern kann.

> ANTWORT MIT SUBSTANZ
>
> Klare Unterscheidung zwischen "zertifiziert", "erfahren in", "orientiert an" und "in Vorbereitung". Verweise auf konkrete Vorgängerprojekte, in denen die Nachweise geliefert wurden.

> WARNZEICHEN
>
> Standards werden pauschal aufgezählt, ohne dass der Anbieter den eigenen Status pro Standard benennen kann.

NEW DIRECTION DAZU: Unsere Standards-Landkarte (Baustein 06 dieser Bibliothek) benennt für jeden Standard den tatsächlichen Status. TISAX zertifiziert. ISO 26262 und Automotive SPICE erfahren in. DO-178C, EMAR, STANAG 4586 orientiert an.

04 Referenzen mit vergleichbarer Kritikalität

PRÜFT: DIE ÜBERTRAGBARKEIT VORHANDENER ERFAHRUNG AUF DEN GEPLANTEN AUFTRAG.

Welche Referenzen aus vergleichbaren Kritikalitäts- und Regulierungsstufen können Sie benennen, und welche davon dürfen offen kommuniziert werden? Ein Anbieter mit ausschließlich zivilen Referenzen mag technisch fähig sein, ist aber ohne Erfahrung in Verwaltungsprozessen und Beschaffungslogik.

> ANTWORT MIT SUBSTANZ
>
> Konkrete Nennung von Kunden und Vertragsformen, klare Trennung zwischen offen zeigbaren und unter Geheimhaltung erwähnbaren Projekten, Übertragbarkeit auf Ihren Auftrag benennbar.

> WARNZEICHEN
>
> Referenzen bleiben vage, Namen werden pauschal geschwärzt, Kritikalitätsstufen werden nicht diskutiert.

NEW DIRECTION DAZU: Öffentlich: BMW EMV seit über 20 Jahren, TÜV Süd, GFAW STAR Systemübernahme, BM-DS Ground Control Station Ghost 150. Anonymisiert: .NET-Fachanwendungen einer nationalen Verteidigung 2024 bis 2028.

05 Vertragsmodelle und Lifecycle-Perspektive

PRÜFT: OB DER ANBIETER IN PROJEKTLAUFZEITEN ODER IN LIFECYCLES DENKT.

Welche Vertragsmodelle bieten Sie für Wartung, Support und Change Requests an, und wie lange betreuen Sie Systeme in der Regel? Softwareverträge im staatlichen und wehrtechnischen Kontext laufen häufig vier bis acht Jahre und benötigen einen Partner, der über diese Zeitspanne stabil liefert.

> ANTWORT MIT SUBSTANZ
>
> Nachweisbare Kundenbeziehungen über zehn oder zwanzig Jahre, standardisierte Wartungsverträge, Change-Request-Prozesse mit dokumentierten Durchlaufzeiten, Obsoleszenz-Management als expliziter Bestandteil.

> WARNZEICHEN
>
> Der Anbieter denkt in Projekten, nicht in Lifecycles. Betreuung endet nach Projektabnahme. Change Requests werden ad hoc verhandelt.

NEW DIRECTION DAZU: Längste laufende Kundenbeziehung 25 Jahre. Wartungs- und Change-Request-Prozesse dokumentiert. Aktuelle Verträge im wehrtechnischen Bereich mit Vier-Jahres-Laufzeit.

06 Reaktionsfähigkeit und Servicequalität

PRÜFT: OB REAKTIONSZEITEN VERBINDLICH DEFINIERT ODER REIN ASPIRATIONAL SIND.

Innerhalb welcher Fristen antworten Sie auf Erstanfragen, wie hoch ist Ihre Reaktionsgarantie bei Störfällen, und über welche Kanäle kommunizieren Sie? Beschaffung im öffentlichen Sektor arbeitet mit klar definierten Reaktionszeiten. Ein Anbieter, der diese nicht offen benennen kann, wird in laufenden Verfahren schnell zum Engpass.

> ANTWORT MIT SUBSTANZ
>
> Zugesagte Erstantwort innerhalb weniger Werktage unter NDA, definierte Servicezeiten mit Personenerreichbarkeit, dedizierte E-Mail-Postfächer für Beschaffer, verschlüsselte Kommunikation auf Anfrage.

> WARNZEICHEN
>
> Reaktionszeiten werden nicht garantiert. Anfragen laufen über allgemeine Vertriebs-Postfächer. Verschlüsselte Kommunikation ist Marketing-Behauptung ohne technische Grundlage.

NEW DIRECTION DAZU: Zugesagte Erstantwort auf Beschaffer-Anfragen innerhalb von fünf Werktagen unter NDA. Dediziertes Postfach getintouchwith@newdirection.de. PGP auf Anfrage. Servicezeiten Mo bis Fr 08 bis 17 Uhr.

07 Sprachkompetenz und Behördenerfahrung

PRÜFT: DIE OPERATIVE SPRACHFÄHIGKEIT IM VERWALTUNGS- UND VERGABEKONTEXT.

Welche Sprachen deckt Ihr operatives Team ab, und welche vergaberechtlichen Prozesse beherrschen Sie? Reibungsverluste durch Sprachbarrieren oder Unkenntnis des Vergaberechts verlangsamen Beschaffungsprozesse erheblich und werden im Zuschlagsverfahren geprüft.

> ANTWORT MIT SUBSTANZ
>
> Muttersprachliche Abdeckung Deutsch und Englisch, für die Schweiz auch Französisch und Italienisch, direkte Erfahrung mit WTO-Vergaben, Selbstdeklaration BKB, Schweizer Beschaffungskonferenz.

> WARNZEICHEN
>
> Kommunikation nur über Vermittler oder externe Übersetzer. Erste Erfahrung mit Vergaberecht steht noch aus.

NEW DIRECTION DAZU: Deutsch, Englisch, Französisch operativ abgedeckt. Ständige Vertretung Schweiz in St. Gallen. Vergabeverfahren im WTO-Bereich zuletzt 2023 erfolgreich absolviert.

08 Exportkontrolle und Compliance

PRÜFT: OB DER ANBIETER DUAL-USE-PRÜFUNG ALS OPERATIVEN PROZESS FÜHRT.

Wie prüfen Sie Ihre Leistungen auf exportkontrollrechtliche Relevanz, und wie ist der interne Prozess bei Dual-Use-Klassifizierung organisiert? Softwarekomponenten im Defence- und High-Tech-Umfeld können unter Verordnung (EU) 2021/821 und das Außenwirtschaftsgesetz fallen.

> ANTWORT MIT SUBSTANZ
>
> Etablierter interner Prüfprozess mit dokumentierter Zuständigkeit, klarer Umgang mit Drittanbieter-Libraries, Beschreibung der Entscheidungslogik bei Auftragsprüfung.

> WARNZEICHEN
>
> Unkenntnis über Dual-Use-Bestimmungen. Berufung auf externe Beratung ohne interne Verantwortung.

NEW DIRECTION DAZU: Interne Compliance-Verantwortung benannt. Jede Anfrage durchläuft eine Exportkontroll-Prüfung. Zuständiger Ansprechpartner: compliance@newdirection.de.

09 Übernahme bestehender Systeme

PRÜFT: DIE FÄHIGKEIT ZUR NAHTLOSEN FORTFÜHRUNG FREMDER CODEBASEN.

Haben Sie Erfahrung darin, ein laufendes System von einem Vorgängerdienstleister zu übernehmen, ohne den Betrieb zu unterbrechen? Selten startet ein Auftrag auf der grünen Wiese. Häufig geht es um die Fortführung eines Systems, das dokumentarisch oder personell dünn übergeben wird.

> ANTWORT MIT SUBSTANZ
>
> Standardisierter Übernahmeprozess, dokumentierte Referenzen für nahtlose Übergänge, Code-Audit- und Refactoring-Strategie ohne Betriebsunterbrechung.

> WARNZEICHEN
>
> Der Anbieter fordert pauschal den Neubau, weil die Einarbeitung in Fremdcode abgelehnt wird.

NEW DIRECTION DAZU: Zwei Systemübernahmen 2023 und 2024 erfolgreich abgeschlossen, davon eine im öffentlichen Sektor. Standardisierter Übernahmeprozess in vier Phasen dokumentiert (Baustein 05 dieser Bibliothek).

10 Eigentümerstruktur und Souveränität

PRÜFT: DIE EIGENTUMSRECHTLICHE KONTROLLE ÜBER QUELLCODE UND DATEN.

Wie ist die Eigentümerstruktur Ihres Unternehmens organisiert, und welche Kontrolle über Quellcode und Daten liegt tatsächlich in Ihrer Hand? Im wehrtechnischen und behördlichen Kontext prüfen Auftraggeber zunehmend die eigentumsrechtliche Souveränität ihrer Lieferanten.

> ANTWORT MIT SUBSTANZ
>
> Klare Auskunft zur Eigentümerstruktur, keine intransparenten Beteiligungen, Quellcode und Datenhaltung im Inland, keine Abhängigkeit von Zulieferern außerhalb des vereinbarten Rechtsraums.

> WARNZEICHEN
>
> Eigentümerstruktur wird bei Rückfragen ausweichend beantwortet. Quellcode oder Daten liegen in wechselnden Cloudregionen.

NEW DIRECTION DAZU: 100 Prozent deutsche Eigner. Keine ausländischen Beteiligungen. Quellcode-Repositories im Inland. Datenhaltung in geprüften deutschen Rechenzentren.

11 Insolvenz-Vorsorge und Fortbestandssicherung

PRÜFT: WAS MIT IHREM SYSTEM PASSIERT, WENN IHR LIEFERANT ZAHLUNGSUNFÄHIG WIRD.

Beschaffungsverfahren betrachten selten die wirtschaftliche Fortbestandslage des Anbieters über die Vertragslaufzeit. Bei sicherheitskritischen Systemen mit langer Bindung kann eine unangekündigte Insolvenz zum Systemstillstand führen. Ein professioneller Anbieter hat für diesen Fall vorgesorgt und macht die Vorsorge transparent.

> ANTWORT MIT SUBSTANZ
>
> Quellcode-Escrow bei einem notariellen Hinterlegungsdienst, vertragliche Regelung zur Weitergabe der Rechte an den Auftraggeber im Insolvenzfall, dokumentierte Übergabe-Prozeduren, Absicherung der Betriebsfähigkeit für mindestens 90 Tage nach Insolvenzanmeldung.

> WARNZEICHEN
>
> Das Thema wird als unwahrscheinlich abgetan, keine Escrow-Regelung, keine dokumentierte Prozedur für den Insolvenzfall, keine belastbare Kapitalstruktur.

NEW DIRECTION DAZU: Escrow-Vereinbarungen mit notariellem Hinterlegungsdienst in Vorbereitung für alle langlaufenden Mandate. Dokumentierte Übergabe-Prozedur. Solide Eigenkapitalbasis. Fortbestand seit 1998.

12

Zugang befristeter Kräfte zu Quellcode und Daten

PRÜFT: DIE GRAUZONE DER ZUGANGSKONTROLLE BEI WERKSTUDENTEN, PRAKTIKANTEN, EXTERNEN BERATERN.

Wie regeln Sie den Zugang von Werkstudentinnen, Praktikantinnen und externen Beratern zu Quellcode und Testdaten in Ihren Aufträgen? Die meisten Zertifizierungen regeln festes Personal. Befristete Kräfte und externe Berater sind oft in einer Grauzone. In sicherheitskritischen Projekten ist genau diese Grauzone das häufigste Einfallstor.

> ANTWORT MIT SUBSTANZ
>
> Klare Regelung zur Sicherheitsüberprüfung befristeter Kräfte, dokumentierte Zugriffsrechte je Rolle, technische Trennung sensibler Bereiche, automatisierte Löschung von Zugängen nach Vertragsende, Onboarding- und Offboarding-Prozeduren.

> WARNZEICHEN
>
> Werkstudenten haben pauschalen Repository-Zugriff, externe Berater arbeiten remote ohne kontrollierten Zugang, keine dokumentierten Prozeduren für Beendigung von Zugängen.

NEW DIRECTION DAZU: Werkstudenten und Praktikanten arbeiten ausschließlich in nicht-klassifizierten Projekten. Rollenbasierte Zugriffsrechte. Automatisierte Offboarding-Prozedur mit Zugangswiderruf am Tag des Ausscheidens.

ZUM WEITEREN AUSTAUSCH

Dieser Guide ist Teil unserer Beschaffer-Bibliothek.

Fünf weitere Dokumente stehen in derselben Bibliothek zum freien Download bereit. Für Rückfragen zu einzelnen Prüfpunkten oder zur Anwendung des Guides auf konkrete Beschaffungsverfahren sind wir unter getintouchwith@newdirection.de innerhalb von fünf Werktagen erreichbar. Auf Wunsch unter beidseitiger Geheimhaltung.

E-MAIL FÜR BESCHAFFER
getintouchwith@newdirection.de

VERTRETUNG SCHWEIZ
St. Gallen · +41 71 45522-57

CONFIDENTIALITY AGREEMENT · VERTRAULICHKEITSVEREINBARUNG

Zweiseitige Vertraulichkeitsvereinbarung.

Vorlage für Erstgespräche und technische Sondierungen zwischen new direction und Beschaffungsstellen, Systemherstellern oder Konsortialpartnern. Bilingual Deutsch und Englisch. Der deutsche Wortlaut ist bei Auslegungsfragen maßgeblich.

VORLAGE	ANWENDUNG	BAUSTEIN	ABSENDER
Bilingual DE/EN	Erstgespräche	02 von 06	new direction GmbH

ZWISCHEN

Anschrift

Vertreten durch

— NACHFOLGEND "PARTEI A" —

UND

new direction GmbH

Hauptstraße 7, 86356 Neusäß

Vertreten durch die Geschäftsführung

— NACHFOLGEND "PARTEI B" —

Die Parteien beabsichtigen, im Rahmen eines Erstgesprächs oder einer technischen Sondierung Informationen auszutauschen, die vertraulicher Natur sind. Zu diesem Zweck vereinbaren sie die folgenden Regelungen. Diese Vorlage stellt einen Musterentwurf dar und ersetzt keine anwaltliche Prüfung im Einzelfall. Sie kann durch die Vorlage der offenlegenden Partei ersetzt werden.

The Parties intend to exchange information of a confidential nature within the scope of an initial meeting or technical exploration. To this end, they agree on the provisions set out below. This template constitutes a draft and does not replace legal review in individual cases. It may be superseded by the disclosing Party's own template.

§ 1 Zweck — *Purpose*

Zweck dieser Vereinbarung ist die Prüfung einer möglichen Zusammenarbeit im Bereich `Projektbezeichnung`. Die im Rahmen dieser Prüfung offengelegten Informationen werden nach Maßgabe dieser Vereinbarung behandelt.

The purpose of this Agreement is the evaluation of a potential cooperation in the field of `[Project Name]`. Information disclosed in the course of this evaluation shall be handled in accordance with this Agreement.

§ 2 Vertrauliche Informationen — *Confidential Information*

Vertrauliche Informationen sind alle technischen, wirtschaftlichen, rechtlichen und sonstigen Angaben, Unterlagen, Quellcodes, Spezifikationen, Kenntnisse und Erkenntnisse, die eine Partei der anderen im Rahmen des Zwecks in schriftlicher, elektronischer, mündlicher oder verkörperter Form offenlegt und die nach Inhalt oder Kennzeichnung als vertraulich erkennbar sind.

Confidential Information means all technical, commercial, legal and other data, documents, source code, specifications, know-how and findings disclosed by one Party to the other in the course of the Purpose in written, electronic, oral or embodied form and which are recognisable as confidential by content or marking.

§ 3 Pflichten der empfangenden Partei — *Obligations of the Receiving Party*

Die empfangende Partei verpflichtet sich,

1. Vertrauliche Informationen ausschließlich für den in § 1 vereinbarten Zweck zu verwenden,
2. sie mit derselben Sorgfalt zu schützen, mit der sie eigene vertrauliche Informationen schützt, mindestens jedoch mit der Sorgfalt eines ordentlichen Kaufmanns,
3. sie nur solchen Mitarbeitenden, Beauftragten oder Beratern zugänglich zu machen, die diese für den Zweck kennen müssen und einer gleichwertigen Vertraulichkeitspflicht unterliegen.

The receiving Party undertakes to

1. use Confidential Information solely for the Purpose defined in Section 1,
2. protect it with the same care as it protects its own confidential information, in any event with the care of a diligent business,
3. disclose it only to employees, agents or advisors who need to know it for the Purpose and who are bound by equivalent confidentiality obligations.

§ 4 Ausnahmen — *Exceptions*

Die Vertraulichkeitspflicht gilt nicht für Informationen, die

1. zum Zeitpunkt der Offenlegung bereits öffentlich bekannt waren oder ohne Verschulden der empfangenden Partei öffentlich bekannt werden,
2. der empfangenden Partei nachweislich bereits vor der Offenlegung bekannt waren,
3. von der empfangenden Partei nachweislich unabhängig ohne Nutzung der Vertraulichen Informationen entwickelt wurden,
4. aufgrund gesetzlicher Vorschriften, behördlicher Anordnung oder rechtskräftiger Entscheidung offengelegt werden müssen, wobei die empfangende Partei die offenlegende Partei unverzüglich informiert.

The confidentiality obligation shall not apply to information that

1. was already publicly known at the time of disclosure or becomes publicly known without fault of the receiving Party,
2. was demonstrably known to the receiving Party prior to disclosure,
3. was demonstrably developed independently by the receiving Party without use of the Confidential Information,
4. must be disclosed by statutory provision, administrative order or final court decision, in which case the receiving Party shall promptly inform the disclosing Party.

§ 5 Weitergabe an Dritte — *Disclosure to Third Parties*

Die Weitergabe Vertraulicher Informationen an Dritte, einschließlich verbundener Unternehmen und Unterauftragnehmer, bedarf der vorherigen schriftlichen Zustimmung der offenlegenden Partei. Die empfangende Partei stellt sicher, dass zugelassene Dritte einer gleichwertigen Vertraulichkeitspflicht unterliegen.

Disclosure of Confidential Information to third parties, including affiliates and subcontractors, requires the prior written consent of the disclosing Party. The receiving Party ensures that approved third parties are bound by equivalent confidentiality obligations.

§ 6 Kein Rechteübergang — *No Transfer of Rights*

Diese Vereinbarung begründet keinen Übergang von Eigentums-, Urheber-, Patent-, Marken- oder sonstigen Schutzrechten. Vertrauliche Informationen verbleiben im Eigentum der offenlegenden Partei.

This Agreement shall not effect any transfer of ownership, copyright, patent, trademark or other intellectual property rights. Confidential Information shall remain the property of the disclosing Party.

§ 7 Laufzeit und Rückgabe — *Term and Return*

Diese Vereinbarung tritt mit beidseitiger Unterzeichnung in Kraft. Die Vertraulichkeitspflicht besteht für die Dauer von `drei Jahren` nach Abschluss der Sondierung oder Beendigung der Zusammenarbeit fort. Auf schriftliche Anforderung der offenlegenden Partei sind Vertrauliche Informationen sowie alle Kopien und Auszüge unverzüglich zurückzugeben oder nachweisbar zu vernichten. Die Vernichtung ist auf Verlangen schriftlich zu bestätigen.

This Agreement enters into force upon mutual signature. The confidentiality obligation shall remain in effect for a period of `three years` after conclusion of the exploration or termination of the cooperation. Upon written request of the disclosing Party, Confidential Information and all copies and excerpts shall be promptly returned or verifiably destroyed. Destruction shall be confirmed in writing upon request.

§ 8 Haftung — *Liability*

Für Schäden aus einer Verletzung dieser Vereinbarung haftet die verletzende Partei nach den gesetzlichen Bestimmungen. Weitergehende Rechte, insbesondere Ansprüche auf Unterlassung, bleiben unberührt. Die Parteien anerkennen, dass eine Verletzung Vertraulicher Informationen zu erheblichen und nicht vollständig durch Geldersatz auszugleichenden Schäden führen kann.

The breaching Party shall be liable for damages resulting from a breach of this Agreement in accordance with statutory provisions. Further rights, in particular claims for injunctive relief, shall remain unaffected. The Parties acknowledge that a breach of Confidential Information may lead to substantial damages that cannot be fully compensated by monetary damages.

§ 9 Anwendbares Recht und Gerichtsstand — *Governing Law and Jurisdiction*

Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist Augsburg.

This Agreement shall be governed by the laws of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods. The exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement shall be Augsburg.

§ 10 Schlussbestimmungen — *Miscellaneous*

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.

Amendments and additions to this Agreement require written form. This applies also to the waiver of the written form requirement. Should any provision of this Agreement be or become invalid, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced by a provision that comes closest to the intended commercial purpose.

UNTERSCHRIFTEN · SIGNATURES

PARTEI A	PARTEI B · NEW DIRECTION GMBH
ORT, DATUM · PLACE, DATE	ORT, DATUM · PLACE, DATE
UNTERSCHRIFT · SIGNATURE	UNTERSCHRIFT · SIGNATURE
NAME, FUNKTION · NAME, TITLE	NAME, FUNKTION · NAME, TITLE

HINWEIS · NOTICE

Diese Vorlage stellt einen Musterentwurf dar. Sie ersetzt keine anwaltliche Prüfung im Einzelfall. Bei Aufträgen mit klassifiziertem Inhalt oder mit Geheimschutz-Relevanz können weitergehende Vereinbarungen erforderlich sein. Die new direction GmbH akzeptiert alternativ die Geheimhaltungsvorlage der offenlegenden Partei. · This template constitutes a draft. It does not replace legal review in individual cases. For engagements with classified content or security clearance relevance, additional agreements may be required. new direction GmbH accepts alternatively the disclosing Party's own non-disclosure template.

LIEFERANTEN-SELBSTAUSKUNFT

Strukturierte Vorlage zur Erstprüfung von Softwarelieferanten.

Die Vorlage vereint die Angaben, die Beschaffer typischerweise abfragen. Die mittlere Spalte zeigt beispielhaft die Angaben von new direction. Die rechte Spalte bleibt für den zu prüfenden Lieferanten leer.

VORLAGE	UMFANG	BAUSTEIN	STAND
Deutsch	8 Bereiche	03 von 06	1 / 2026

BEREICH 01 · GRUNDDATEN

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Firmierung, Rechtsform	*new direction GmbH*	
Sitz und Handelsregister	*Neusäß, HRB Augsburg*	
Gründungsjahr	*1998*	

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Weitere Standorte	*Zweigniederlassung St. Gallen, Schweiz*	
Umsatzsteuer-ID	*DE…*	

BEREICH 02 · EIGENTUM UND STRUKTUR

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Eigentümerstruktur	*100 % deutsche Eigner, keine ausländischen Beteiligungen*	
Konzernzugehörigkeit	*Nein, eigenständig*	
Geschäftsführung	*Michael Robert Biber, Stephan Weber*	
Beteiligungen an Dritten	*Keine*	

BEREICH 03 · PERSONAL

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Anzahl Mitarbeitende (Stichtag)	*Rund 30, davon Engineering-Team am Standort Neusäß*	
Anteil Festangestellte	*Über 90 Prozent*	
Sicherheitsüberprüftes Personal	*Im Rahmen laufender Mandate, Ausweitung in Vorbereitung*	
Sprachkompetenz operativ	*Deutsch, Englisch, Französisch*	
Längste Betriebszugehörigkeit	*Über 24 Jahre*	

BEREICH 04 · REFERENZEN

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Aktuelles Aerospace-Mandat	*Ground Control Station Ghost 150, BM-DS AG*	
Aktuelles Defense-Mandat	*.NET-Fachanwendungen einer nationalen Verteidigung, 2024 bis 2028*	
Aktuelles Public-Sector-Mandat	*Weiterentwicklung System STAR, GFAW Thüringen*	
Längste Industriebeziehung	*BMW Group, über 20 Jahre (EMV-Messdaten)*	
Weitere Referenzen	*TÜV Süd, Audi, SIXT, Europcar, AL-KO, APZ, RENK*	

BEREICH 05 · ZERTIFIZIERUNGEN UND STANDARDS

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
TISAX	*Zertifiziert, Ablauf 2028*	
EcoVadis	*Gold, aktuell*	

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
ISO 27001	*In Vorbereitung*	
Domänen-Standards	*Siehe Baustein 06 Standards-Landkarte*	
Forschungssiegel Stifterverband	*"Innovativ durch Forschung"*	

BEREICH 06 · COMPLIANCE UND STEUERN

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Steuer- und Sozialabgabenstatus	*Keine Rückstände, Unbedenklichkeitsbescheinigung auf Anfrage*	
Exportkontroll-Prozess	*Interner Prüfprozess nach EU 2021/821 und AWG etabliert*	
Selbstdeklaration BKB	*Erfüllt*	
Selbstdeklaration Schweiz	*Erfüllt gemäß Schweizer Beschaffungskonferenz*	
Compliance-Ansprechpartner	*compliance@newdirection.de*	

BEREICH 07 · FORTBESTAND UND KONTINUITÄT

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Quellcode-Escrow	*In Vorbereitung für alle langlaufenden Mandate*	
Business Continuity	*Dokumentierte Übergabe-Prozedur, Betriebsfähigkeit 90 Tage nach Insolvenz*	
Wirtschaftsprüfer	*Auf Anfrage*	
Berufshaftpflichtversicherung	*Bestehend, Deckungsangaben auf Anfrage*	

BEREICH 08 · KONTAKT FÜR BESCHAFFUNG

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Beschaffer-Postfach	*getintouchwith@newdirection.de*	
Erstantwort-SLA	*Fünf Werktage unter NDA*	
Servicezeiten	*Mo bis Fr 08 bis 17 Uhr*	

ANGABE	NEW DIRECTION (BEISPIEL)	IHR UNTERNEHMEN
Verschlüsselte Kommunikation	*PGP auf Anfrage*	

SECURITY QUESTIONNAIRE

Antwortmuster für Security-Fragebögen von Primes und Beschaffern.

Die Vorlage folgt der Struktur von ISO 27001 Anhang A. Sie umfasst zehn Kernbereiche und liefert Referenzantworten, die als Ausgangspunkt für die Bearbeitung individueller Fragebögen dienen. Die Antworten sind sachlich, ohne Auftragsspezifika.

STRUKTUR	UMFANG	BAUSTEIN	STAND
ISO 27001 Anhang A	10 Bereiche	04 von 06	1 / 2026

Auftraggeber im wehrtechnischen und im behördlichen Kontext versenden typischerweise mehrseitige Security Questionnaires, bevor eine tiefere Zusammenarbeit beginnt. Diese Fragebögen unterscheiden sich in Länge und Detailtiefe, folgen aber in den Bereichen einer wiederkehrenden Struktur.

Die folgenden zehn Bereiche entsprechen den zentralen Domänen von ISO 27001 Anhang A und decken die Prüf-Themen ab, die in den meisten Fragebögen vorkommen. Zu jedem Bereich formulieren wir eine Referenzantwort, wie new direction sie in einem Erstkontakt liefert.

A.5

Informationssicherheitsrichtlinien

Verfügt Ihr Unternehmen über eine dokumentierte Informationssicherheits-Richtlinie? Wer verantwortet sie? Wann wurde sie zuletzt überarbeitet?

REFERENZANTWORT

Ja. Verabschiedet und regelmäßig überprüft durch die Geschäftsführung, letzte Überarbeitung im Rahmen der TISAX-Auditierung 2025. Kernrichtlinie ergänzt durch spezifische Verfahrensanweisungen für Entwicklung, Zugriff und Vorfallsmanagement.

A.6

Organisation der Informationssicherheit

Wer trägt die operative Verantwortung für Informationssicherheit? Wie sind Rollen und Trennung von Aufgaben geregelt?

REFERENZANTWORT

Benannter Informationssicherheitsbeauftragter mit direkter Berichtslinie an die Geschäftsführung. Trennung von operativen und prüfenden Rollen. Externe Auditbegleitung durch TISAX-akkreditierten Prüfdienstleister.

A.7

Personalsicherheit

Wie werden Beschäftigte und externe Kräfte vor Aufnahme der Tätigkeit geprüft? Wie erfolgt Onboarding und Offboarding hinsichtlich Zugängen und Verpflichtungen?

REFERENZANTWORT

Führungs- und polizeiliche Führungszeugnisse für sicherheitsrelevante Rollen. Sicherheitsüberprüfungen für Personal in klassifizierten Mandaten. Achtstündiges Sicherheits-Onboarding für alle neuen Kräfte. Automatisierte Offboarding-Prozedur mit Zugangswiderruf am Tag des Ausscheidens.

A.8

Asset-Management

Wie werden Informationswerte identifiziert, klassifiziert und dem Verantwortlichen zugeordnet? Wie werden Klassifizierungsstufen technisch umgesetzt?

REFERENZANTWORT

Zentraler Asset-Katalog mit Klassifizierung nach Vertraulichkeit, Integrität, Verfügbarkeit. Klassifizierung folgt den Anforderungen der Auftraggeber. Umsetzung in Zugriffsrechten, Verschlüsselung und Backup-Regimen.

A.9

Zugriffskontrolle

Wie wird der Zugriff auf Systeme und Informationen gewährt und regelmäßig geprüft? Wie sind privilegierte Zugriffe kontrolliert?

REFERENZANTWORT

Rollenbasierte Zugriffssteuerung. Mehrfaktor-Authentisierung für alle kritischen Systeme. Quartalsweise Rezertifizierung der Berechtigungen. Privilegierte Zugriffe zeitlich befristet und protokolliert.

A.10

Kryptographie

Welche kryptographischen Verfahren werden eingesetzt? Wie erfolgt Schlüsselmanagement?

REFERENZANTWORT

Ausschließlich Verfahren nach BSI TR-02102 und aktuellen Empfehlungen. Symmetrisch AES-256, asymmetrisch RSA-4096 oder elliptische Kurven. Zentrales Schlüsselmanagement mit dokumentiertem Lebenszyklus.

A.11

Physische Sicherheit

Wie ist die physische Sicherheit der Betriebsstätten organisiert? Zugangskontrollen, Videoüberwachung, Besucherregelung?

REFERENZANTWORT

Sicherheitsüberprüfter Standort in Augsburg mit Zugangskontrolle, dokumentierter Besucherregelung, Videoüberwachung öffentlicher Bereiche. Serverräume separat gesichert. Reinigungspersonal unter Verschwiegenheitsverpflichtung.

A.12

Betriebssicherheit

Wie erfolgen Patch-Management, Malware-Schutz und Sicherung? Welche Logs werden geführt und wie lange aufbewahrt?

REFERENZANTWORT

Automatisiertes Patch-Management, kritische Sicherheits-Patches innerhalb definierter Fristen. Endpoint-Protection auf allen Systemen. Backup-Konzept nach 3-2-1-Regel mit Offline-Kopie. Log-Aufbewahrung mindestens ein Jahr, sicherheitsrelevante Ereignisse länger.

A.14

Anwendungssicherheit

Wie ist Security in den Entwicklungsprozess integriert? Code-Reviews, statische Analyse, Testabdeckung, Freigabeprozesse?

REFERENZANTWORT

Security by Design als Prozessvorgabe. Vier-Augen-Prinzip bei Code-Reviews. Statische Analyse in der CI-Pipeline. Dependency-Scanning für Open-Source-Komponenten. Test-Coverage nach Kritikalität, dokumentierte Freigabepfade für Releases.

A.16

Vorfallsmanagement

Wie werden Sicherheitsvorfälle erkannt, gemeldet und bearbeitet? Welche Meldefristen gelten gegenüber Auftraggebern?

REFERENZANTWORT

Dokumentierter Incident-Response-Prozess. Meldung an Auftraggeber innerhalb der vertraglich vereinbarten Fristen, in der Regel innerhalb von 24 Stunden bei sicherheitsrelevanten Vorfällen. Post-Incident-Reviews mit Ableitung von Maßnahmen.

A.17

Business Continuity

Welche Vorkehrungen bestehen für den Fortbestand der Leistungsfähigkeit? Recovery-Ziele, Redundanzen, Insolvenz-Vorsorge?

REFERENZANTWORT

Dokumentiertes Business-Continuity-Konzept. Redundante Entwicklungsumgebungen. Recovery-Ziele nach Auftrag definiert. Quellcode-Escrow in Vorbereitung. Betriebsfähigkeit 90 Tage nach Insolvenzanmeldung dokumentiert.

A.18

Compliance

Welche gesetzlichen und vertraglichen Anforderungen werden systematisch überwacht? Wie erfolgt der Nachweis?

REFERENZANTWORT

Compliance-Register mit den relevanten Vorschriften (DSGVO, EU 2021/821, AWG, TISAX-Vorgaben, branchenspezifische Standards). Regelmäßige interne Prüfungen. Externe Audits durch TISAX und EcoVadis. Compliance-Ansprechpartner: compliance@newdirection.de.

ANWENDUNG DIESER VORLAGE

Diese Antwortvorlage ist Ausgangspunkt, kein fertiger Fragebogen.

Jeder Auftraggeber verwendet einen eigenen Fragebogen mit spezifischen Formulierungen und Zusatzfragen. Die Referenzantworten dieser Vorlage dienen als Baseline, die auf die konkrete Fragestellung angepasst werden muss. Für auftragsspezifische Anpassungen, insbesondere bei klassifizierten Mandaten, sind wir unter getintouchwith@newdirection.de erreichbar.

COMPLIANCE-ANSPRECHPARTNER
compliance@newdirection.de

BESCHAFFER-POSTFACH
getintouchwith@newdirection.de

Vier Phasen für die Übernahme eines Systems von einem Vorgängerdienstleister.

Praxisleitfaden für nahtlose Übergaben ohne Betriebsunterbrechung. Entstanden aus zwei Systemübernahmen der Jahre 2023 und 2024, davon eine im öffentlichen Sektor.

STRUKTUR	UMFANG	BAUSTEIN	STAND
Vier Phasen	Etwa 30 Prüfpunkte	05 von 06	1 / 2026

Die Übernahme eines laufenden Systems von einem Vorgängerdienstleister ist einer der schwierigsten Momente eines langfristigen Softwareauftrags. Die Fallhöhe ist hoch, weil ein Fehler in der Übernahme über Jahre wirkt. Die Sichtbarkeit ist gering, weil externe Beobachter das eigentliche Handwerk nicht sehen.

Diese Checkliste gliedert den Übernahmeprozess in vier Phasen mit klaren Prüfpunkten. Sie ist im Kern eine Betriebsanleitung für Beschaffungsverantwortliche, die einen Anbieterwechsel begleiten müssen. Sie kann parallel vom scheidenden und vom übernehmenden Anbieter genutzt werden.

01 Vor der Übernahme (Due Diligence)

ZEITFENSTER: 4 BIS 6 WOCHEN VOR ÜBERGABE

- [ ] Vollständigkeit der Übergabe-Dokumentation prüfen (Architektur, Betriebshandbuch, Datenmodell, Schnittstellen)
  Fehlende Dokumentation ist der häufigste Fund. Frühe Aufnahme im Übergabe-Protokoll schafft Verbindlichkeit.
- [ ] Repository-Status und Zugangswege identifizieren (Git-Historie, Branches, Tags, Vollständigkeit)
  Ein unvollständiges Repository, das nur ausgeliefert und nicht historisiert übergeben wird, blockiert langfristige Wartung.
- [ ] Ticket-Historie sichten und Change-Request-Backlog übergeben
  Offene Tickets aus der Ära des Vorgängers zeigen die tatsächlichen Systemschwächen.
- [ ] Vertragsbeziehungen zu Zulieferern und Drittkomponenten identifizieren
  Vergessene Zulieferer-Verträge sind eine typische Kostenfalle im ersten Betriebsjahr.
- [ ] Lizenzen und Nutzungsrechte prüfen (Open Source, Kommerz, Auftragsrechte)
  Vom Vorgänger unter proprietärer Lizenz eingesetzte Bibliotheken müssen dokumentiert übergeben werden.
- [ ] Technische Schuld inventarisieren und mit dem Auftraggeber priorisieren
  Ehrliche Aufnahme technischer Schuld verhindert Überraschungen im dritten Betriebsjahr.

02 Übergabe-Zeitraum

ZEITFENSTER: 4 BIS 8 WOCHEN PARALLEL

- [ ] Parallelbetrieb definieren (Zuständigkeiten, Meldewege, Freigabepfade)
  Wer entscheidet in der Übergangsphase über Change Requests? Klare Regelung schriftlich fixieren.
- [ ] Wissenstransfer-Sessions mit Schlüsselpersonen des Vorgängers durchführen
  Aufzeichnung der Sessions unter beidseitiger Zustimmung reduziert spätere Rückfragen.
- [ ] Kommunikationskanäle etablieren und Ansprechpartner benennen
  Der Auftraggeber muss zu jedem Zeitpunkt wissen, wen er anspricht.
- [ ] Test-Umgebungen aufbauen und mit produktiver Umgebung abgleichen
  Divergenzen zwischen Test und Produktion sind Standardfehler bei Systemübernahmen.
- [ ] Erste eigene Change Requests umsetzen, um das System aus Anwendersicht zu verstehen
  Ein simulierter kleiner Change Request in der Übergabephase deckt Prozesslücken auf.

03 Übernahme

ZEITFENSTER: STICHTAG DER VERANTWORTUNGSÜBERNAHME

- [ ] Alle Zugangsdaten rotieren (Datenbanken, Systeme, externe Dienste)
  Der Vorgänger darf nach dem Stichtag keinen operativen Zugriff mehr haben.
- [ ] Deployment-Pipelines übernehmen und auf eigene Infrastruktur umstellen
  Pipelines des Vorgängers sind oft an dessen CI/CD-Landschaft gebunden. Frühe Migration reduziert Ausfallrisiko.
- [ ] Backup- und Restore-Prozeduren testen und dokumentieren
  Ein Restore-Test in der ersten Woche der Übernahme zeigt sofort, ob die übergebenen Backups nutzbar sind.
- [ ] Monitoring und Alerting auf eigene Systeme umstellen
  Blackouts entstehen häufig, weil Alerts noch auf den Vorgänger geroutet werden.
- [ ] Betriebshandbücher aktualisieren und Kommunikationswege final freigeben
  Auftraggeber und weitere Beteiligte müssen die neuen Kontaktdaten schriftlich erhalten.

04 Nach der Übernahme

ZEITFENSTER: ERSTE 30, 90 UND 180 TAGE

- [ ] Erste 30 Tage: engmaschiges Monitoring, tägliche Statusprüfung
  Systemstabilität ist noch nicht garantiert. Fehler aus der Übergabephase kommen jetzt zutage.
- [ ] Erste 90 Tage: erste eigene Change Requests umsetzen und Reaktionszeiten validieren
  Der Auftraggeber prüft in dieser Phase, ob die zugesagten Servicezeiten realistisch sind.
- [ ] Erste 180 Tage: Retrospektive gemeinsam mit Auftraggeber
  Eine dokumentierte Retrospektive nach sechs Monaten ist der beste Vertrauensanker für die kommenden Vertragsjahre.
- [ ] Verbleibende offene Punkte aus der Übernahme abschließen
  Punkte, die in der Übergabephase auf "später" verschoben wurden, drohen sonst dauerhaft offen zu bleiben.

ERGÄNZUNG DIESER CHECKLISTE

Die Checkliste basiert auf zwei Systemübernahmen.

Wir haben 2023 die Übernahme des Systems STAR von einem Vorgängerdienstleister im Auftrag der GFAW Thüringen ohne Betriebsunterbrechung durchgeführt. Wir haben 2024 im Rahmen eines WTO-Vergabeverfahrens .NET-Fachanwendungen einer nationalen Verteidigung übernommen. Beide Übernahmen haben die hier aufgeführten Prüfpunkte hervorgebracht. Für Anwendungsfragen zu dieser Checkliste sprechen Sie uns an.

BESCHAFFER-POSTFACH
getintouchwith@newdirection.de

VERTRETUNG SCHWEIZ
St. Gallen · +41 71 45522-57

STANDARDS-LANDKARTE

Ehrliche Statusangabe pro Standard.

Übersicht der Standards, an denen new direction arbeitet, mit klarer Kennzeichnung des tatsächlichen Status. Diese Landkarte ist die Grundlage der Aussagen im Beschaffer-Guide, in der Selbstauskunft und im Security Questionnaire.

UMFANG	AKTUALISIERUNG	BAUSTEIN	STAND
8 Standards	Quartalsweise	06 von 06	1 / 2026

Anbieter im wehrtechnischen und behördlichen Kontext neigen dazu, alle Standards, mit denen sie in Berührung gekommen sind, gleichrangig aufzuzählen. Das schafft

Verwirrung. Ein Beschaffer kann anhand einer solchen Aufzählung nicht mehr erkennen, worauf er sich verlassen kann.

Wir differenzieren pro Standard nach fünf Status-Stufen. Diese Differenzierung ist bewusst restriktiv. Eine Aufnahme in "Zertifiziert" erfolgt nur, wenn ein aktuelles Zertifikat vorliegt. Eine Aufnahme in "Erfahren in" nur, wenn wir konkrete Projekte nachweisen können.

STANDARD	DOMÄNE	STATUS BEI NEW DIRECTION
TISAX	Informationssicherheit im Automotive-Umfeld	Zertifiziert
EU 2021/821	Dual-Use-Verordnung	Eingehalten
ISO 26262	Funktionale Sicherheit Automotive	Erfahren in
Automotive SPICE	Reifegrad Software Automotive	Erfahren in
DO-178C	Software in der zivilen Luftfahrt	Orientiert an
EMAR	Militärische Lufttüchtigkeit	Orientiert an
STANAG 4586	UAV-Interoperabilität	Orientiert an
ISO 27001	Informationssicherheits-Managementsystem	In Vorbereitung

Zertifiziert. Aktuelles Zertifikat einer akkreditierten Prüfstelle liegt vor. Auf Anfrage geben wir Ausstellungs- und Ablaufdatum bekannt.

Eingehalten. Gesetzliche Anforderungen werden im Rahmen etablierter interner Prozesse laufend erfüllt.

Erfahren in. Wir haben in konkreten Projekten die zugehörigen Nachweise (Traceability, Testabdeckung, Dokumentation) erbracht.

Orientiert an. Wir richten unsere Arbeit an der Methodik des Standards aus, sind aber nicht zertifiziert und liefern keine förmlichen Konformitätsnachweise.

In Vorbereitung. Ein Auditverfahren ist angestoßen oder eine Prozessvorbereitung läuft. Konkrete Angaben zum Stand geben wir auf Anfrage.

HINWEIS ZUR AKTUALISIERUNG

> Diese Landkarte wird quartalsweise aktualisiert. Änderungen im Status kommunizieren wir aktiv an Auftraggeber laufender Mandate. Für Beschaffer im aktiven Angebotsverfahren teilen wir auf Anfrage schriftliche Bestätigungen zum Status ausgewählter Standards mit.