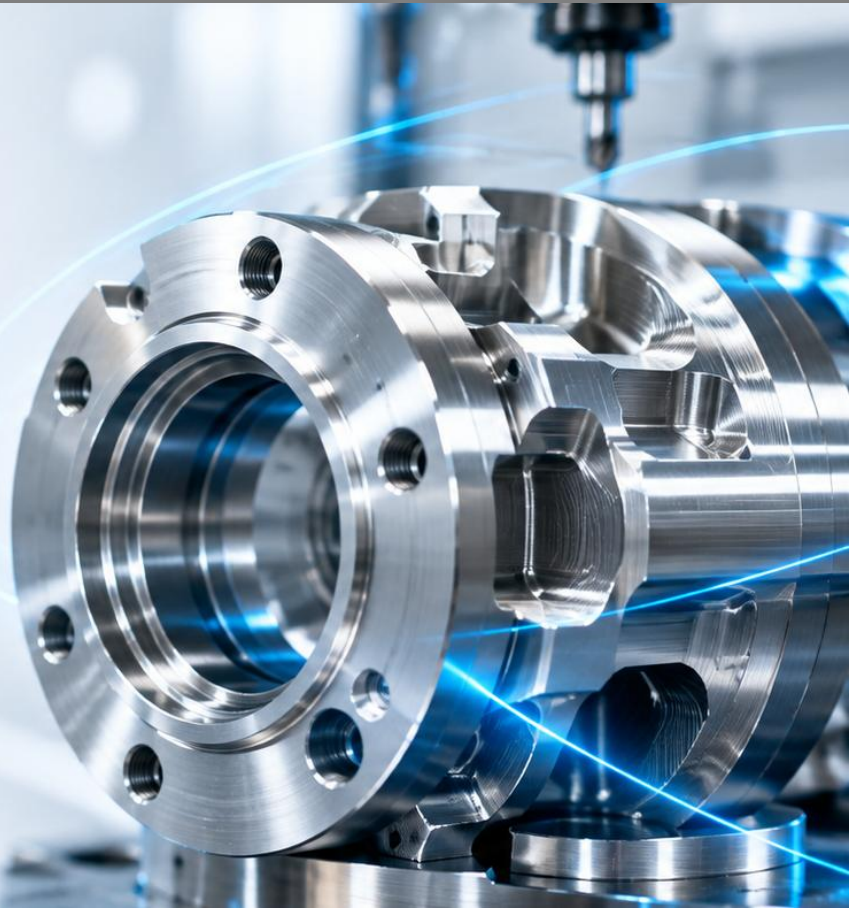
Metallkongress 2026

Metallkongress 2026

Risiken im Zulieferbetrieb

Cybersicherheit und Daten
Verträge, Haftung und Zahlung



Christian Derr
Dr. Stefan Zipse

Leitfaden: zwei Bereiche

01 Christian Derr

Cybersicherheit und Daten

- NIS-2 und Cyber Resilience Act
- Fernwartung und Updates
- Data Act und Datenrechte
- Schutz von Geschäftsgeheimnissen

02 Dr. Stefan Zipse

Verträge und Haftung

- Kundenbedingungen und QSV
- Haftung und Produkthaftung
- Zahlungsausfall und Insolvenz
- Vertragliche Absicherung

Cybersicherheit und Maschinendaten

NIS-2 und Cyber Resilience Act

Data Act und vertragliche Datennutzung

Christian Derr

Datenschutz und Compliance

Betrieb, Produkt und Daten

NIS-2

- IT und Produktion
- Tätigkeit und Größe
- Geschäftsleitung
- BSI-Meldungen

CRA

- Produktsicherheit
- Digitale Elemente
- Herstellerpflichten
- Updates

Data Act

- Maschinendaten
- Nutzerrechte
- Nutzungsverträge
- Geheimnisschutz

§§ 28–38 BSIG; Art. 2, 13–14 CRA; Art. 3–7 Data Act. DSGVO bei Personenbezug zusätzlich

Praxisfall: vernetzte CNC-Fertigung

Eine Maschine, mehrere Beteiligte

1
Betrieb
Nutzer

2
Hersteller
Fernwartung

3
IT-Partner
Infrastruktur

4
Abnehmer
Qualitätsdaten

Fernwartung, Updates und Datenzugriff

NIS-2: direkte Betroffenheit

1. Tätigkeit: z. B. Maschinenbau (NACE 28)
2. ≥ 50 Beschäftigte ODER Umsatz UND Bilanz > 10 Mio. €
3. Unternehmensgruppe und Tätigkeit mitprüfen

NACE 25 allein: keine automatische NIS-2-Pflicht

§ 28 Abs. 2–4 BSIG, Anlage 2 Nr. 5. Tätigkeit und Größe müssen zusammen passen

NIS-2: Verantwortung der Geschäftsleitung

Geschäftsleitung

- Umsetzung
- Überwachung
- Regelmäßige Schulung

1. Risikoanalyse
2. Budget und Verantwortung
3. Kontrollen und Nachweise
4. Registrierung beim BSI
5. Krisenübung und Kontakte

§§ 30, 33, 38 BSIG. Pflichten nach § 38 für unmittelbar erfasste Einrichtungen

Cybersicherheit in Kundenverträgen

Sicherheitsniveau

Konkrete TOM

Nachweise

Prüfumfang, Audits

Meldewege

Auslöser, Fristen

Unterlieferanten

Pflichten weitergeben

Updates

Support, Zuständigkeit

Haftung

Erfüllbare Zusagen

§ 30 Abs. 2 Nr. 4 BSIG. TOM = technische und organisatorische Maßnahmen. Vertragsdetails in den Notizen

CRA: digitale Produkte und Herstellerpflichten

Herstellerrolle

Eigene digitale Produkte

Produktbezug

Steuerung, Firmware

Größe

Auch kleine Hersteller

Seit 11.09.2026

Meldepflichten

Ab 11.12.2027

Produktpflichten, CE

Lebenszyklus

Support und Updates

Art. 2–3, 13–14, 69 und 71 CRA, VO (EU) 2024/2847. Ausnahmen produktbezogen prüfen

Fernwartung: Zugriff unter Kontrolle

1. Persönliche Konten und MFA
2. Freigabe je Wartungseinsatz
3. Begrenzte Rechte und Zugriffszeit
4. Protokollierung und Abschaltung

Im Vertrag

- Erlaubte Systeme
- Erlaubte Tätigkeiten
- Supportstandorte
- Notfallkontakt

§ 30 Abs. 2 Nr. 4–5 und 9–10 BSIG; Art. 28 und 32 DSGVO, soweit anwendbar. MFA = Mehrfaktor-Authentifizierung

Updates und IT-Dienstleister

Updates

- Verantwortung
- Supportdauer
- Test und Freigabe
- Sicherung, Rückfallplan

IT-Dienstleister

- Leistungsumfang
- Aktuelle TOM
- Unterauftragnehmer
- Nachweise und Exit

Sicherheitsvorfall: Meldewege und Fristen

Regime	Auslöser	Erste Fristen
NIS-2	Erheblicher Vorfall	24 h / 72 h
CRA	Ausnutzung / Vorfall*	24 h / 72 h
DSGVO	Datenpanne mit Risiko	Möglichst 72 h
IT-Dienstleister	Datenpanne als AV	Unverzüglich
Kundenvertrag	Vereinbarter Auslöser	Vertragsfrist

Interne Sofortmeldung und parallele Meldewege

§ 32 BSIG; Art. 14 CRA; Art. 33 DSGVO. Ab Kenntnis. *CRA: aktive Ausnutzung / schwerwiegender Produktvorfall

Data Act: Datenumfang und Geltung

Erfasste Daten

- Rohdaten
- Vorverarbeitung
- Metadaten
- Zustandsdaten

Abgrenzung

- Vernetzte Produkte
- Verbundene Dienste
- CAD und Analysen: gesonderte Prüfung

Zeit und Größe

- Seit 12.09.2025
- Design: Neuprodukte nach 12.09.2026
- Art. 7: Ausnahmen

Art. 2–7 und 50 Data Act, VO (EU) 2023/2854. Kein pauschaler Anspruch auf sämtliche Betriebsdaten

Datenrechte an der CNC-Maschine

Nutzer

- Datenzugang
- Unentgeltlich
- Drittanbieter wählen

Dateninhaber

- Daten bereitstellen
- Eigennutzung: Vertrag erforderlich
- Schutzkonzept

Serviceanbieter

- Auf Nutzerwunsch
- Vereinbarter Zweck
- Löschung nach Zweck

Art. 4–6 und 8–9 Data Act. Herstellerrolle und Dateninhaberschaft sind gesondert zu prüfen

Vereinbarungen zur Datennutzung

Datenumfang

Felder, Metadaten

Zweck

Wartung, Qualität

Zugang

Format, Schnittstelle

Weitergabe

Empfänger, Grenzen

Schutz

TOM, Vertraulichkeit

Vertragsende

Export, Löschung

Art. 3–6, 8–9 und 13 Data Act; bei Auftragsverarbeitung zusätzlich Art. 28 DSGVO

Datenzugang und Geschäftsgeheimnisse

Geheimnisse konkret benennen und wirksam schützen

1
Daten klassifizieren

2
Zugriff begrenzen

3
NDA vereinbaren

4
Schutz nachweisen

Datenverweigerung: nur unter engen Voraussetzungen

§ 2 Nr. 1 GeschGehG; Art. 4 Abs. 6–9 und Art. 5 Abs. 9–12 Data Act. NDA = Vertraulichkeitsvereinbarung

Personenbezug in Maschinendaten

1. Bediener- und Supportdaten
2. Rechtsgrundlage und Information
3. Verantwortlicher oder Auftragsverarbeiter
4. Drittlandzugriff und Löschfristen

IT-Vertrag

- Rollen vor Vertrag
- AVV, soweit nötig
- Aktuelle TOM
- Supportstandorte

Art. 1 Abs. 5 Data Act; Art. 5–6, 13–14, 28, 32 und 44 ff. DSGVO; ggf. § 26 BDSG

Maßnahmen für die nächsten 30 Tage

1. Betroffenheit klären
2. Risiken priorisieren
3. Fernzugänge prüfen
4. Wiederherstellung testen
5. Meldewege festlegen
6. IT-Verträge aktualisieren
7. Updatepflichten zuordnen
8. Datenrechte vereinbaren
9. Geheimnisse schützen
10. Geschäftsleitung schulen

Praxisempfehlung zur Priorisierung. Gesetzliche und vertragliche Fristen gelten unabhängig davon

Risiken als Zulieferer: Verträge, Haftung, Zahlungsausfall

Welche Risiken Zulieferer tragen und wie sie sie begrenzen

Dr. Stefan Zipse, Rechtsanwalt
Arbeitskreis Feinwerkmechaniker

Ablaufplan: drei Risikofelder in 30 Minuten

I **Bedingungen Ihrer Kunden**
Einkaufsbedingungen · QSV · Änderungen

II **Ihre Haftung als Zulieferer**
Reklamation · Stillstand · Produkthaftung

III **Wenn der Kunde nicht zahlt**
Vorsorge · Lieferstopp · Insolvenz

✓ **Checkliste**
Zehn Punkte für die Praxis

Kundenbedingungen: Was gilt für Sie?

1. B2B: Hinweis auf die AGB genügt (§ 310 BGB)
2. AGB widersprechen sich: Gesetz gilt (§ 306 BGB)
3. QSV unterschrieben: Kundenbedingungen gelten

Vor der Unterschrift prüfen und verhandeln

Diese Klauseln verlagern Risiken auf Sie

Wareneingang

Rügepflicht auf Sie verlagert

Verjährung

36 statt 24 Monate

Pauschalen

Kosten ohne Verschulden

Garantien

Haftung ohne Verschulden

Rückruf

Kosten ohne Obergrenze

Dokumentation

15 Jahre und mehr

Vertragsstrafe und Garantie: Was Sie zusagen

Vertragsstrafe

- Höchstens 5 % des Auftrags
- Nur bei Verschulden
- Anrechnung auf Schaden
- Keine Herabsetzung (§ 348 HGB)

Garantie

- Haftung ohne Verschulden
- Kein Haftungsdeckel (§ 444 BGB)
- Besser: Beschaffenheit vereinbaren
- ppm-Ziel ist keine Garantie

Der Kunde ändert den Auftrag

Kein einseitiges Änderungsrecht: Ihre Zustimmung ist Ihr Hebel

1
Änderung schriftlich

2
Nachtrag: Preis, Termin

3
Auftrag vor Ausführung

4
Aufwand belegen

Mengen

- Forecast ist kein Abruf

Preise

- Materialpreisgleitklausel

Reklamation: Was zahlen Sie als Zulieferer?

Kosten	Grundlage	Verschulden?
Nacharbeit, Ersatz	§ 439 Abs. 1, 2 BGB	nein
Aus- und Einbau	§ 439 Abs. 3 BGB	nein
Sortierung	§ 280 BGB	ja, vermutet
Stillstand	§ 280 BGB	ja, vermutet
Rückruf	§§ 280, 823 BGB	ja

QSV: oft Pauschalen ohne Verschulden

Stillstand beim Kunden: Wann haften Sie?

1. Ihr Teil ist mangelhaft oder zu spät
2. Ihr Verschulden wird vermutet
3. Ausfallschaden ohne Mahnung
4. Mitverschulden des Kunden?

Was hilft

- Haftungshöchstbetrag
- Zieltermine
- Früh informieren
- Versicherung

Ihre Haftung wirksam begrenzen

Nie begrenzbar

- Vorsatz, grobe Fahrlässigkeit
- Personenschäden
- Produkthaftung
- Garantien

In AGB möglich

- Einfache Fahrlässigkeit: typischer Schaden
- Unwesentliche Pflichten

Nur individuell

- Fester Höchstbetrag
- Keine Folgeschäden
- Verhandlung belegen

Produkthaftung neu: Folgen für Zulieferer

Software

auch Firmware und Updates

Direkte Haftung

als Hersteller von Komponenten

Ab 9.12.2026

für neu gelieferte Produkte

Keine Obergrenze

Regress des Kunden steigt

Beweislast

Offenlegung, Vermutungen

Bis 25 Jahre

bei Spätschäden

Ihr Geld sichern: vor der Lieferung

Anzahlung

- Nur wenn vereinbart
- Deckt Material

Meilensteine

- An Ereignisse knüpfen
- Feste Termine
- Lange Ziele begrenzt

Sicherheiten

- Eigentums-vorbehalt
- Bürgschaft
- Kredit-versicherung

Kunde zahlt schleppend: Lieferstopp?

§ 321 BGB: Vorleistung verweigern, wenn Zahlung gefährdet

1
Warnsignale belegen

2
Vorkasse verlangen

3
Frist setzen

4
Rücktritt

Unberechtigter Lieferstopp ist selbst Vertragsbruch

Wenn der Kunde insolvent wird

Anfechtung droht

- 3 Monate bei Kenntnis
- Bis 4 Jahre bei Vorsatz
- Raten allein schaden nicht

Schutz

- Bargeschäft: Zug um Zug
- Eigentumsvorbehalt
- Lösungsklausel unwirksam

Kundenspezifische Teile und Anlagen

Ihr Risiko

- Kein Zweitmarkt
- Nach Einbau kein Eigentum
- Freie Kündigung (§ 648 BGB)

1. Anzahlung 30–50 %
2. Meilensteinplan
3. Freigaben schriftlich
4. Stornoregel
5. Zeichnungen erst nach Zahlung

Checkliste für die Praxis

1	QSV vorher verhandeln
2	Back-to-back absichern
3	Keine Garantien
4	Vertragsstrafe deckeln
5	Änderung nur mit Nachtrag
6	Haftung deckeln
7	Produkthaftung vorbereiten
8	Anzahlung vereinbaren
9	§ 321 BGB nutzen
10	Krise: Zug um Zug

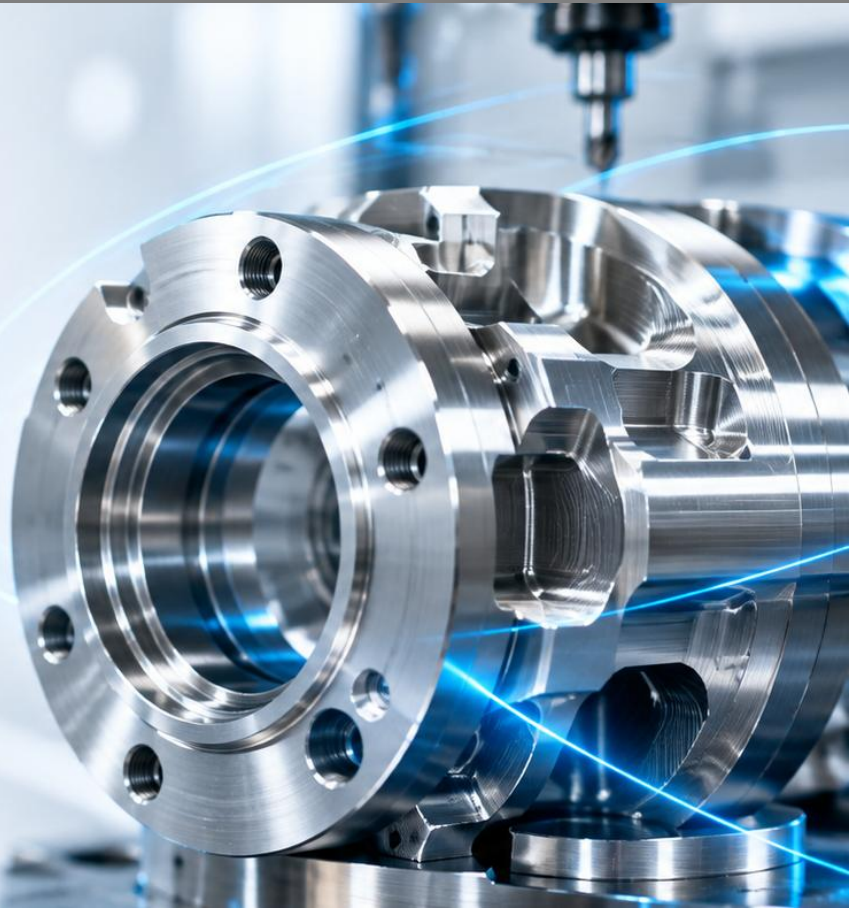
Metallkongress 2026

Metallkongress 2026

Vielen Dank

Offene Fragen und Austausch

Christian Derr
Dr. Stefan Zipse



Ihre Ansprechpartner

Christian Derr

Datenschutz und Compliance

www.derr-ponte.de

Dr. Stefan Zipse

Rechtsanwalt

www.kanzlei-zipse.de

Scannen und Kontakt speichern