Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

(Stand 10/2024)

Zwischen

Auftraggeber
(im Folgenden "Verantwortlicher")

Und

P3N AG
Crimmitschauer Straße 32, 08412 Werdau
vertreten durch den Vorstand: Thomas Birnstein und Joachim Becker
(im Folgenden "Auftragsverarbeiter")

1. Gegenstand und Dauer des Auftrags

1.1. Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen Hauptvertrag zwischen den Parteien. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen und nach dessen Weisung gemäß Art. 28 DSGVO.

1.2. Die Dauer der Auftragsverarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Eine Beendigung der Auftragsverarbeitung erfolgt mit der Beendigung des Hauptvertrags oder nach Weisung des Verantwortlichen.

2. Art der Verarbeitung und Datenkategorien

2.1. **Art und Zweck**: Die Art und der Zweck der Verarbeitung personenbezogener Daten ergeben sich aus dem Hauptvertrag.

2.2. **Datenkategorien**: Die Verarbeitung umfasst insbesondere Kunden-, Mitarbeiter- und Lieferantendaten des Verantwortlichen.

2.3. **Betroffene Personen**: Betroffen sind insbesondere Kunden, Mitarbeiter und Lieferanten des Verantwortlichen.

3. Rechte und Pflichten des Verantwortlichen

3.1. Der Verantwortliche ist verantwortlich für die Rechtmäßigkeit der Datenverarbeitung und erteilt dem Auftragsverarbeiter die erforderlichen Weisungen.

3.2. Der Verantwortliche hat das Recht, die Einhaltung der vertraglichen und gesetzlichen Datenschutzvorschriften zu überprüfen, einschließlich der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters.

4. Pflichten des Auftragsverarbeiters

4.1. **Verarbeitung auf Weisung**: Der Auftragsverarbeiter verarbeitet die Daten nur gemäß den Weisungen des Verantwortlichen. Er wird den Verantwortlichen informieren, wenn eine Weisung gegen geltendes Recht verstößt.

4.2. **Vertraulichkeit**: Der Auftragsverarbeiter stellt sicher, dass alle Personen, die Zugang zu personenbezogenen Daten haben, zur Vertraulichkeit verpflichtet sind.

4.3. **Sicherheit der Verarbeitung**: Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein angemessenes Schutzniveau sicherzustellen. Die Maßnahmen werden regelmäßig überprüft und angepasst, um den aktuellen Stand der Technik zu gewährleisten. Eine Dokumentation der Maßnahmen wird dem Verantwortlichen auf Anfrage zur Verfügung gestellt.

4.4. **Unterauftragsverhältnisse**: Der Auftragsverarbeiter darf Unterauftragnehmer nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen einsetzen. Die Datenschutzstandards müssen dabei eingehalten werden, und die Einhaltung durch Unterauftragnehmer wird regelmäßig überprüft.

4.5. **Unterstützung bei Betroffenenrechten**: Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Betroffenenrechte, insbesondere bei Auskunfts-, Löschungs- und Berichtigungsanfragen.

4.6. **Meldung von Datenschutzverletzungen**: Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 72 Stunden, über Verstöße gegen den Schutz personenbezogener Daten und dokumentiert alle relevanten Details der Verletzung.

4.7. **Löschung und Rückgabe von Daten**: Nach Beendigung der Auftragsverarbeitung werden die Daten nach Wahl des Verantwortlichen gelöscht oder zurückgegeben. Die Löschung der Daten erfolgt innerhalb einer vom Verantwortlichen festgelegten, angemessenen Frist nach Beendigung des Auftragsverhältnisses, es sei denn, gesetzliche Aufbewahrungspflichten bestehen. In diesem Fall erfolgt die Löschung nach Ablauf der Aufbewahrungspflichten.

4.8. **Internationale Datenübermittlungen**: Datenübermittlungen in Drittstaaten außerhalb der EU oder des EWR dürfen nur erfolgen, wenn die Voraussetzungen der Art. 44-49 DSGVO erfüllt sind (z. B. durch Standardvertragsklauseln oder Angemessenheitsbeschlüsse).

5. Kontrolle und Nachweispflichten

Der Verantwortliche hat das Recht, die Einhaltung der vereinbarten Datenschutzmaßnahmen durch den Auftragsverarbeiter zu überprüfen. Der Auftragsverarbeiter stellt dafür alle erforderlichen Informationen zur Verfügung. Der Verantwortliche kann Einsicht in die getroffenen technischen und organisatorischen Maßnahmen nehmen und regelmäßige Kontrollen, inklusive Audits, durchführen.

6. Schlussbestimmungen

6.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

6.2. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

Für den Auftragsverarbeiter:

Frank Hummel
Prokurist P3N AG

Für den Auftraggeber:

Anlage 1: Technische und organisatorische Maßnahmen (TOM) (Stand: 10/2024)

Der Auftragsverarbeiter trifft gemäß Art. 32 DSGVO angemessene technische und organisatorische Maßnahmen, um den Schutz der personenbezogenen Daten sicherzustellen. Diese Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten, die Art, den Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

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

- **Zutrittskontrolle**:
  - Zutritt zu den Betriebsräumen nur für berechtigte Personen.
  - Zutritt zu sensiblen Bereichen (z. B. Serverräume) nur für autorisierte Personen.
- **Zugangskontrolle**:
  - Individuelle Benutzerkonten und sichere Passwörter gemäß den jeweils aktuellen Sicherheitsstandards (z. B. BSI-Richtlinien oder anderen anerkannten Branchenstandards).
  - Der Auftragsverarbeiter verpflichtet sich, die Passwortsicherheits-richtlinien regelmäßig an den Stand der Technik anzupassen.
  - Zwei-Faktor-Authentifizierung (2FA) für den Zugang zu sensiblen Systemen.
  - Externe Zugriffe über gesicherte VPN-Verbindungen, die protokolliert werden.
- **Zugriffskontrolle**:
  - Rollen- und Berechtigungskonzept nach dem Prinzip der minimalen Berechtigung.
  - Regelmäßige Überprüfung und Anpassung der Berechtigungen.
  - Technische Maßnahmen zur Zugriffskontrolle (z. B. marktübliche Sicherheitssysteme).
- **Trennungskontrolle**:
  - Getrennte Verarbeitung von Daten in Produktions- und Testsystemen.
  - Mandantendaten werden in separaten Datenbanken oder Verzeichnissen verarbeitet.
- **Pseudonymisierung**:
  - Pseudonymisierung personenbezogener Daten, sofern technisch möglich, mit strikter Trennung von Identifikationsdaten und personenbezogenen Daten.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**:
  - Verschlüsselung personenbezogener Daten bei der Übertragung sowie auf mobilen Datenträgern gemäß den jeweils aktuellen, anerkannten Verschlüsselungsstandards.

    - Der Auftragsverarbeiter stellt sicher, dass die eingesetzten Verschlüsselungstechnologien regelmäßig überprüft und an den Stand der Technik angepasst werden.
    - Mechanische Zerstörung von Datenträgern vor der Entsorgung und Vernichtung von Papierdokumenten nach DIN 66399.
    - Regelmäßige Überprüfung und Auditierung der verschlüsselten Kommunikation.

- **Eingabekontrolle**:
    - Protokollierung von Datenveränderungen, Eingaben und Löschungen durch Benutzer in sensiblen Systemen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- **Verfügbarkeitskontrolle**:
    - Schutz durch Firewalls, Virenscanner, SPAM-Filter und regelmäßige Datensicherungen.
    - Speicherung der Backups an sicheren und geografisch getrennten Standorten.
- **Notfallwiederherstellung**:
    - Regelmäßige Tests der Notfallpläne und Wiederherstellungsverfahren (mindestens jährlich), um die schnelle Wiederherstellung von Daten im Notfall sicherzustellen.
    - Dokumentation der Sicherungsverfahren und Überprüfung der Wiederherstellbarkeit.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- **Datenschutz-Management**:
    - Regelmäßige Überprüfung der Datenschutzmaßnahmen durch interne und externe Audits.
    - Bestellung eines Datenschutzbeauftragten, der für die Überwachung der Maßnahmen zuständig ist.
    - Dokumentation und Auswertung von Datenschutzvorfällen, um kontinuierliche Verbesserungen sicherzustellen.
- **Incident-Response-Management**:
    - Etabliertes Krisenmanagement für den Umgang mit Datenschutzverletzungen, einschließlich der Meldung an den Verantwortlichen innerhalb von 72 Stunden gemäß Art. 33 DSGVO.

Anlage 2: Liste der Unterauftragnehmer

Im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO werden ggf. Unterauftragnehmer durch den Auftragsverarbeiter P3N AG zur Durchführung spezifischer Verarbeitungstätigkeiten eingesetzt.

Bedingungen für den Einsatz von Unterauftragnehmern:

1. **Einbindung des Verantwortlichen**: Der Verantwortliche wird mindestens 14 Tage im Voraus schriftlich über die geplante Einbindung eines neuen Unterauftragnehmers informiert. Der Verantwortliche hat das Recht, der Beauftragung des neuen Unterauftragnehmers innerhalb von zwei Wochen nach Erhalt der Mitteilung ohne Angabe von Gründen zu widersprechen.

2. **Datenschutzkonformität**: Jeder Unterauftragnehmer wird vertraglich verpflichtet, die gleichen Datenschutzstandards wie der Auftragsverarbeiter einzuhalten, insbesondere im Hinblick auf die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Der Auftragsverarbeiter stellt sicher, dass die Unterauftragnehmer die erforderlichen Garantien zum Schutz der personenbezogenen Daten bieten.

3. **Vertragliche Bindung**: Vor der Beauftragung eines Unterauftragnehmers schließt der Auftragsverarbeiter mit diesem einen Auftragsverarbeitungsvertrag ab, der die Anforderungen des Art. 28 DSGVO erfüllt.

4. **Kontrolle**: Der Auftragsverarbeiter überprüft regelmäßig, ob die Unterauftragnehmer die vertraglich vereinbarten Datenschutzmaßnahmen einhalten. Der Verantwortliche kann auf Anfrage die relevanten Auszüge des Vertrags zwischen dem Auftragsverarbeiter und dem Unterauftragnehmer einsehen.

5. **Drittstaatentransfers**: Sollte ein Unterauftragnehmer außerhalb der EU oder des EWR (Drittstaaten) personenbezogene Daten verarbeiten, stellt der Auftragsverarbeiter sicher, dass die entsprechenden Voraussetzungen der Art. 44–49 DSGVO (z. B. Angemessenheitsbeschluss, Standardvertragsklauseln) erfüllt sind.

Ergänzungen und Aktualisierungen:

Die Liste der Unterauftragnehmer wird regelmäßig überprüft und bei Änderungen an den Verantwortlichen übermittelt. Mögliche Ergänzungen und Aktualisierungen erfolgen unaufgefordert.