VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DS-GVO

für die StahlID der Salzgitter Flachstahl GmbH

1. GEGENSTAND UND DAUER DES AUFTRAGS

(1) Diese Vereinbarung ist Bestandteil der Beauftragung zwischen der Salzgitter Flachstahl GmbH (nachfolgend „Auftraggeber") und dem Vertragspartner (nachfolgend „Auftragnehmer"), welcher in der vertraglichen Beauftragung des Auftraggebers oder der sonstigen vertraglichen Vereinbarung zwischen Auftraggeber und Auftragnehmer über die Beauftragung, die auf diese Vereinbarung zur Auftragsverarbeitung verweist, genannt ist. Diese Vereinbarung ergänzt die vertragliche Vereinbarung zwischen Auftraggeber und Auftragnehmer und legt die Bedingungen für die Verarbeitung personenbezogener Daten des Auftragnehmers durch den Auftraggeber im Zusammenhang mit der Verwendung der StahlID fest.

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der vertraglichen Vereinbarung, in dessen Rahmen das StahlID-System genutzt wird.

2. KONKRETISIERUNG DES AUFTRAGSINHALTS

(1) Die Datenverarbeitung durch den Auftraggeber in der StahlID erfolgt zum Zwecke der elektronischen Erfassung der Anwesenheiten von Fremdfirmenmitarbeitern auf dem Gelände der Salzgitter Flachstahl GmbH für eine elektronische Abrechnung der beauftragten Leistungen.

(2) Die Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftragnehmers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(3) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Name, Telefon, E-Mail, Verbindungsdaten)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐

(4) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

- ☒ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Angehörige von Beschäftigten
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☒ Dienstleister
- ☐ Mitarbeiter von Behörden
- ☐ Ansprechpartner
- ☐ Angehörige von Beschäftigten
- ☒ Lieferanten
- ☐

(5) Die Daten dürfen nur für den Zweck verwendet werden, für den Sie erhoben worden sind (Zweckbindung). Die Grundsätze der Datenvermeidung und Datensparsamkeit sind durch die Vertragspartner zu beachten.

3. TECHNISCH-ORGANISATORISCHE MASSNAHMEN

(1) Der Auftraggeber hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dokumentiert und dem Auftragnehmer zur Prüfung übergeben. Durch die Akzeptanz des Auftragnehmers sind die dokumentierten Maßnahmen Grundlage des Auftrags. Der Auftraggeber hat diese Maßnahmen umgesetzt und wendet sie während des Auftrags an. Soweit eine Überprüfung einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftraggeber stellt die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO sicher. Insgesamt handelt es sich bei den Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei berücksichtigt der Auftraggeber den Stand der Technik, die Implementierungskosten und die Art, den Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftraggeber gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

(1) Der Auftraggeber wird die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftragnehmers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftraggeber wendet, wird der Auftraggeber dieses Ersuchen unverzüglich an den Auftragnehmer weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftragnehmers unmittelbar durch den Auftraggeber sicherzustellen.

5. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

Der Auftraggeber sicher zusätzlich zu der Einhaltung der Regelungen dieses Auftrags die gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO ein. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Webseite des Auftraggeber leicht zugänglich hinterlegt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftraggeber wird bei der Durchführung der Arbeiten nur Beschäftigte einsetzen, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftraggeber und jede unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftragnehmer verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftragnehmers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftraggeber ermittelt.

SZFG KM 12/25 AVV_StahlID_1 20251203

SALZGITTER FLACHSTAHL
Ein Unternehmen der Salzgitter Gruppe

Salzgitter Flachstahl GmbH / Eisenhüttenstraße 99 / 38239 Salzgitter
TEL +49 (0) 53 41 21 28 90 / **MAIL** flachstahl@salzgitter-ag.de
www.salzgitter-flachstahl.de

(6) Soweit der Auftragnehmer seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, sichert der Auftraggeber zu, ihn nach besten Kräften zu unterstützen.

(7) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftragnehmer im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. UNTERAUFTRAGSVERHÄLTNISSE

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftraggeber z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftraggeber sichert jedoch zu, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftragnehmers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber ist generell berechtigt, Unterauftragnehmer mit der Verarbeitung zu beauftragen, sofern es sich um verbundene Unternehmen des Auftraggebers im Sinne von § 15 Aktiengesetz handelt.

(3) Der Auftragnehmer stimmt der Beauftragung der in der Anlage „Unterauftragnehmer" benannten Unterauftragnehmer zu. Der Auftraggeber wird vor einer Beauftragung von Unterauftragnehmern stets die Voraussetzungen nach Maßgabe von Art. 28 Abs. 2-4 DS-GVO prüfen und beachten.

(4) Vor einer weiteren Beauftragung auf Unterauftragnehmer oder einem Wechsel bestehender Unterauftragnehmer wird der Auftraggeber den Auftragnehmer schriftlich oder in Textform mindestens dreißig (30) Kalendertage im Voraus informieren. Der Auftragnehmer kann gegen die Beauftragung eines neuen Unterauftragnehmers innerhalb von fünfzehn (15) Tagen nach Kenntnisnahme Einspruch einlegen. Der Auftragnehmer muss nachvollziehbar seinen Einspruch begründen, warum der Auftraggeber den Unterauftragnehmer nicht einsetzen soll. Erfolgt ein rechtzeitiger und ausreichend begründeter Einspruch, versuchen die Parteien die Gründe für den Einspruch gemeinsam zu beseitigen, zum Beispiel durch die Ergreifung weiterer, angemessener Maßnahmen. Erfolgt kein fristgemäßer begründeter Einspruch, ist der Auftraggeber berechtigt, den Unteraufragnehmer zu beauftragen.

(5) Der Auftraggeber wird die vertraglichen Vereinbarungen mit Unterauftragnehmern so gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Unterauftragnehmer sind insbesondere zur Verschwiegenheit und auf das Datengeheimnis zu verpflichten. Eine Weitergabe personenbezogener Daten darf erst nach Vorliegen aller Voraussetzungen erfolgen.

(6) Der Auftraggeber trägt bei Verarbeitungen außerhalb der EU / des EWR für ein angemessenes Datenschutzniveau durch geeignete Garantien, z.B. den Abschluss von EU-Standardvertragsklauseln oder vergleichbarer Regelungen im Rahmen der Unterbeauftragung Sorge.

7. KONTROLLRECHTE DES AUFTRAGGEBERS

(1) Der Auftragnehmer hat das Recht, im Benehmen mit dem Auftraggeber Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Eine Überprüfung ist rechtzeitig vorab anzukündigen, darf nur zu üblichen Geschäftszeiten erfolgen und den Geschäftsbetrieb des Auftraggebers nicht unangemessen beeinträchtigen. Eine Überprüfung ist maximal einmal pro Vertragsperiode zulässig.

(2) Im Falle einer Überprüfung stellt der Auftraggeber sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftraggeber wird erforderliche Auskünfte erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Auftraggeber ist berechtigt, den Nachweis solcher Maßnahmen anstelle einer Vor-Ort-Kontrolle durch die Vorlage geeigneter aktueller Testats, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder geeigneter Zertifizierungen durch IT-Sicherheits- oder Datenschutzaudits – z.B. nach BSI-Grundschutz oder ISO 27001 – („Prüfbericht") zu erbringen, wenn der Prüfbericht es dem Auftragnehmer ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu diesem Vertrag zu überzeugen.

8. MITTEILUNGS- UND UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftraggeber wird den Auftragnehmer unverzüglich nach Kenntnisnahme informieren, wenn durch ihn oder die bei ihm beschäftigte Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind oder ein dahingehender Verdacht besteht.

(2) Der Auftraggeber unterstützt den Auftragnehmer bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich zu melden

c) die Verpflichtung, dem Auftragnehmer im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftragnehmers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftragnehmers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(3) Es ist bekannt, dass im Falle der Auftragsverarbeitung gesetzliche Informationspflichten des Auftraggebers gegenüber der zuständigen Aufsichtsbehörde und den betroffenen Personen im Falle der unrechtmäßigen Übermittlung oder Kenntniserlangung von bestimmten personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder bei anderen Unregelmäßigkeiten im Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen zu ergreifen. Soweit den Auftraggeber gesetzliche Meldepflichten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

(4) Sofern die Unterstützungsleistungen des Auftraggebers ein übliches und angemessenes Maß überschreiten, ist der Auftraggeber berechtigt, für die Erbringung seiner Unterstützungsleistungen eine angemessene Vergütung zu fordern. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

(1) Die Verarbeitung der Daten im Rahmen von Auftragsverarbeitungen erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftragnehmers. Dem Auftragnehmer steht im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung und der geltenden datenschutzrechtlichen Bestimmungen ein Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung zu, welches er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und

SZFG KM 12/25 AVV_StahlID_1 20251203

Salzgitter Flachstahl GmbH / Eisenhüttenstraße 99 / 38239 Salzgitter
TEL +49 (0) 53 41 21 28 90 / **MAIL** flachstahl@salzgitter-ag.de
www.salzgitter-flachstahl.de

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DS-GVO

für die StahlID der Salzgitter Flachstahl GmbH

Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftraggeber grundsätzlich nur nach vorheriger Zustimmung durch den Auftragnehmer erteilen.

(2) Mündliche Weisungen wird der Auftragnehmer unverzüglich schriftlich, per Telefax oder per E-Mail zu wiederholen, um sie zu dokumentieren.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltende Datenschutzvorschriften. Der Auftraggeber ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftragnehmer bestätigt oder geändert wird.

(4) Beide Parteien benennen sich gegenseitig weisungsberechtigte Personen. Änderungen dieser weisungsberechtigten Personen sind dem jeweiligen anderen Vertragspartner in Textform mitzuteilen

10. LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

(1) Kopien oder Duplikate der Daten werden nur im Rahmen der ordnungsmäßen Verarbeitung erstellt, z.B. in Form von technischen Zwischenspeicherungen oder Sicherheitskopien, die zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen und Beendigung der Verarbeitung der Daten des Auftragnehmers im StahlID-System wird der Auftraggeber die Datenbestände wie im entsprechenden Löschkonzept beschrieben löschen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftraggeber entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. SCHLUSSBESTIMMUNG

(1) Beide Parteien verpflichten sich, unabhängig bestehender gesonderter Geheimhaltungsvereinbarungen, über alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse, insbesondere über die bekannt gewordenen Daten, unter Beachtung des Betriebs- und Geschäftsgeheimnisses Stillschweigen zu bewahren. Diese Verpflichtung gilt auch nach Ende des Vertragsverhältnisses fort.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – unwirksam sein oder werden oder die Vereinbarung eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt. Das Gleiche gilt für den Fall einer Lücke.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel.

(4) Es gilt deutsches Recht.

Anlage Technisch-organisatorische Maßnahmen

Anlage Unterauftragnehmer

Anlage Weisungsberechtigte/Weisungsempfänger

SZFG KM 12/25 AVV_StahlID_1 20251203

Salzgitter Flachstahl GmbH / Eisenhüttenstraße 99 / 38239 Salzgitter
TEL +49 (0) 53 41 21 28 90 / **MAIL** flachstahl@salzgitter-ag.de
www.salzgitter-flachstahl.de

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DS-GVO

für die StahlID der Salzgitter Flachstahl GmbH

ANLAGE: UNTERAUFTRAGNEHMER

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma (Unterauftragnehmer)	Anschrift/Land	Leistung
Salzgitter Digital Solutions	Eisenhüttenstraße 99	Support, Hosting
Support, Hosting	38239 Salzgitter	

ANLAGE: WEISUNGSBERECHTIGE/WEISUNGSEMPFÄNGER

1. Weisungsberechtigte Personen des Auftraggebers sind:

Name	Telefon	E-Mail
Elias Pietsch	+49 5341 21-7911	pietsch.e@salzgitter-ag.de

2. Weisungsempfänger des Auftragnehmers sind:

Name	Telefon	E-Mail

SZFG KM 12/25 AVV_StahlID_1 20251203

Salzgitter Flachstahl GmbH / Eisenhüttenstraße 99 / 38239 Salzgitter
TEL +49 (0) 53 41 21 28 90 / **MAIL** flachstahl@salzgitter-ag.de
www.salzgitter-flachstahl.de