Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DS-GVO

Zwischen

- Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO - nachstehend Auftraggeber genannt -

und

PROMESS GmbH
Energiemesstechnik
Röntgenstr. 1/1
73730 Esslingen am Neckar

- Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO - nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Leistungsvereinbarung Abrechnungs- oder Werkverträgen oder in anderen Leistungsverträgen in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand, Art und Zweck des Auftrags ergibt sich aus den Leistungsvereinbarungen, insbesondere:

- Ablesen von Mess- und Erfassungsgeräten
- Wartung und Austausch von Mess- und Erfassungsgeräten
- Wartung und Austausch von Rauchwarnmeldern
- Erstellung von Heiz- und Betriebskostenabrechnungen
- Breitstellung von Daten über geschützte Systeme (Internet, Apps, etc.)

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

(2) Dauer

Die Gültigkeit dieser Vereinbarung (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Darüberhinausgehende Verarbeitungen von personenbezogenen Daten durch den Auftragnehmer, beispielweise aufgrund von gesetzlichen Aufbewahrungspflichten und Betroffenenrechten, unterliegen weiterhin den Vorgaben der DS-GVO sowie nationalen Bestimmungen.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich 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 Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Findet eine Verarbeitung in einem Drittland statt, sind das Land und die Gewährleistung des angemessenen Schutzniveaus in der Anlage 2 aufgeführt.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Kundendaten
- Lieferantendaten
- Mitarbeiterdaten
- Personenbezogene Daten für Geschäftszwecke
- Besondere Arten personenbezogener Daten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden, Wohnungseigentümer, Mieter
- Lieferanten
- Interessenten
- Mitarbeiter
- Dritte

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden 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 sind der Stand der Technik, die Implementierungskosten und die Art, der 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. Die Maßnahmen sind vom Auftragnehmer in Anlage 1 dieser Vereinbarung aufzuführen und konkret zu beschreiben.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer 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 Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenübertragbarkeit und Auskunft nach Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung die gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO zu erfüllen; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Die Kontaktdaten sind in Anlage 1 Punkt 4 aufgeführt.

aa) Falls der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union, aufgeführt in Anlage 1 Punkt.

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

c) 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 [Dokumentation in Anlage 1].

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

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

e) Die unverzügliche Information des Auftraggebers 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 Auftragnehmer ermittelt.

f) Soweit der Auftraggeber 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, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

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

i) Der Auftragnehmer führt gemäß Art. 30 Abs. 2 DS-GVO ein Tätigkeitsverzeichnis und stellt dieses auf Anforderung des Auftraggebers diesem zur Verfügung.

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 Auftragnehmer 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 Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Auslagerung auf Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers sind zulässig, soweit:

eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, gilt Punkt 2, Abs. 1 dieses Vertrags.

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig, wenigstens 7 Werktage vorher, anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz). Die Kontrollrechte aus Punkt 7, Abs. 1 bleiben davon unberührt.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 30 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören insbesondere:

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 an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber 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 Auftraggebers für dessen Datenschutz-Folgenabschätzung

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

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Eine schriftliche Bestätigung der Löschung ist auf Anforderung auszustellen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Für den Auftraggeber:

_____, den _____ _____

Für den Auftragnehmer:

Esslingen_____, den _____

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle:
  - Elektronische Zutrittskontrolle mit Codekarten oder Schließzylindern

- Zugangskontrolle:
  - Passwortgeschütze Benutzerprofile
  - Zuordnung von Benutzerprofilen zu IT-Systemen
  - Gesperrte Schnittstellen (z.Bsp. USB-Schnittstellen)
  - hard- und softwaregestütze Firewall
  - Verschlüsselte Verbindungen
  - Anti-Viren-Software

- Zugriffskontrolle
  - Zugriffskontrolle über Benutzerprofile
  - Logdateien zur Kontrolle und Überwachung
  - Automatische Sperrung bei fehlender Authentifikation

- Trennungskontrolle
  - Daten werden entsprechend des Auftrages getrennt gespeichert
  - Alle Mitarbeiter sind angewiesen und geschult, Daten nur im Rahmen der Leistungserbringung und zur Wahrung der Zweckbindung zu erheben, zu verarbeiten und zu nutzen
  - Der Auftragnehmer nutzt personenbezogene Daten nur für interne Zwecke im Rahmen des Auftrages oder der Kundenbeziehung

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  - Verschlüsselung von Dateninhalten
  - Protokollierung des Versand
  - Einsatz geprüfter und zertifizierter Versandmedien und Versanddienstleiste

- Eingabekontrolle

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz

- Zugriffskontrolle über Benutzerprofile
- Logdateien zur Kontrolle und Überwachung
- Automatische Sperrung bei fehlender Authentifikation

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  - Mehrfache Sicherung auf geschützte Server
  - Sicherung der Sicherungsserver auf mobile Datenträger (verschlüsselt) zur Aufbewahrung außerhalb der Geschäftsräume
  - Eine unterbrechungsfreie Stromversorgung (USV) ist vorhanden
  - Serverräume sind klimatisiert
  - Warnsysteme (Temperatur, etc) sind installiert
    Feuerlöscher für elektrische Systeme sind vorhanden

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - Verfahren für eine rasche Wiederherstellbarkeit sind vorhanden

4. Datenschutz-Management

- Verantwortliche Ansprechpartner:

  Markus Strauss
  tacticx GmbH
  Walbecker Str. 53
  47608 Geldern

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Incident-Response-Management;

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- Auftragskontrolle

  Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Handelsregister Stuttgart HRB 9469 · Sitz der Gesellschaft ist in Esslingen am Neckar · USt-Id-Nr. DE147823094
Geschäftsführer: Sven Kazenmaier, Manuela Schulz