Ergänzende Vertragsbedingungen zur Auftragsverarbeitung gem. Art. 28 DSGVO

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Auftragnehmer erbringt Leistungen in Zusammenhang mit gebäudetechnischen Systemen (Installations-, Störungsbeseitigungs-, Inbetriebsetzungs-, Datensicherungs-, Wartungs-, Inspektions- und/oder Instandsetzungsleistungen) für den Auftraggeber und ggfls. Kunden des Auftraggebers, vor Ort oder im Wege des Fernzugriffs. Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen Vertrag (im Folgenden „Leistungsvereinbarung“) in den diese Leistungsvereinbarung, auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“). Diese Ergänzenden Vertragsbedingungen zur Auftragsverarbeitung legen die Pflichten der Parteien hinsichtlich der Verarbeitung personenbezogener Daten im Zusammenhang mit dem Auftrag fest.

1.2 Dauer

Die Dauer des Auftrags und die Laufzeit dieser Vereinbarung entsprechen der Laufzeit der Leistungsvereinbarung. Die Parteien können ihre Rechte ausüben, solange der Auftragnehmer personenbezogene Daten für den Auftraggeber im Zusammenhang mit dem Auftrag verarbeitet.

1.3 Recht zur außerordentlichen Kündigung

Jede der Parteien kann die Leistungsvereinbarung sowie die Vereinbarung jederzeit mit angemessener Frist aus wichtigem Grund kündigen, wenn die andere Partei eine erhebliche Pflichtverletzung nach dieser Vereinbarung begeht.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum („EWR“) statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

2.2 Art der Daten

Gegenstand der Verarbeitung sind folgende Datenarten/-kategorien:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefonnummern, E-Mail-Adressen)
- Abrechnungsrelevante Zeiterfassungsdaten
- Zutrittsberechtigungen
- Zeitbuchungen
- Zutrittsbuchungen
- Zutritts- und Zeiterfassungsdaten

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte des Auftraggebers
- Beschäftigte von Fremdfirmen
- Besucher in den Räumlichkeiten des Auftraggebers

3. Technisch-organisatorische Maßnahmen

3.1

Der Auftragnehmer hat die Sicherheit der Verarbeitung gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO zu gewährleisten, indem er die technischen und organisatorischen Maßnahmen gemäß Anlage 1 trifft und aufrechterhält. 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 DSGVO zu berücksichtigen.

3.2

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. Umsetzung von Betroffenenrechten

4.1

Erhält der Auftraggeber Anfragen oder Mitteilungen von betroffenen Personen in Bezug auf die Verarbeitung personenbezogener Daten, unterstützt der Auftragnehmer den Auftraggeber auf dessen Anweisung in angemessener Weise und liefert ihm auf Anfrage entsprechende Informationen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2

Auf Weisung des Auftraggebers hat der Auftragnehmer personenbezogene Daten zu korrigieren, zu löschen oder zu sperren.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer

Herr Norbert Hermkes
c/o dormakaba International Holding GmbH
DORMA Platz 1
58256 Ennepetal

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) 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 im Zusammenhang mit dieser Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) 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.

6. Unterauftragsverhältnisse

6.1

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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen.

6.2

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur unter den folgenden Voraussetzungen beauftragen.

a) Der Auftraggeber stimmt der Beauftragung verbundener Unternehmen im Sinne der §§ 15 ff. AktG sowie der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragsnehmer	Leistung	Anschrift/Land
keine		

b) Die Beauftragung weiterer Unterauftragnehmer und/oder der Wechsel bestehender Unterauftragnehmer sind zulässig, soweit:

- der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab unter Angabe des geplanten Auslagerungstermins anzeigt (mind. Textform) und
- der Auftraggeber nicht bis spätestens 4 Wochen vor dem mitgeteilten, geplanten Auslagerungstermins gegenüber dem Auftragnehmer in Textform begründet Einspruch gegen die geplante Auslagerung erhebt, weil die Beauftragung des Unterauftragnehmers gegen diese Vereinbarung oder anwendbares Datenschutzrecht verstößt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zwischen dem Auftragnehmer und dem Unterauftragnehmer zugrunde gelegt wird.

6.3

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

6.4

Im Falle eines begründeten Einspruchs des Auftraggebers gegen die Beauftragung eines weiteren Unterauftragnehmers oder den Wechsel eines bestehenden Unterauftragnehmers kann der Auftragnehmer die Leistung gegenüber dem Auftraggeber innerhalb von 4 Wochen nach Zugang des Einspruchs einstellen und die Leistungsvereinbarung fristlos und mit sofortiger Wirkung kündigen, sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist.

6.5

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6.6

Eine Auslagerung durch den Unterauftragnehmer auf einen weiteren Auftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Auftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind, soweit möglich, auch dem weiteren Auftragsverarbeiter aufzuerlegen.

7. Kontrollrechte des Auftraggebers

7.1

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

7.2

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.3

Soweit erforderlich hat der Auftraggeber das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende, hinreichend zur Geheimhaltung verpflichtete Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden und während der normalen Geschäftszeiten durchzuführen sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer vor Ort in dessen Geschäftsbetrieb zu überzeugen. Dabei sind anlassunabhängige Kontrollen auf max. eine Kontrolle je Vertragsjahr beschränkt.

7.4

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen, soweit dies im Hauptvertrag entsprechend geregelt ist.

8. Unterstützung des Auftraggebers

8.1

Der Auftragnehmer unterstützt den Auftraggeber 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 vorherigen 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 an den Auftraggeber zu melden,
c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber der zuständigen Behörde und/oder der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
d) die Unterstützung des Auftraggebers bei dessen verpflichtenden Datenschutz-Folgenabschätzungen, und
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen soweit dies im Hauptvertrag entsprechend geregelt ist.

9. Weisungsbefugnis des Auftraggebers

9.1

Vorbehaltlich entgegenstehender gesetzlicher Verpflichtungen verarbeitet der Auftragnehmer die personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Für Weisungen, die zu einer Verarbeitung außerhalb des Geltungsbereichs dieser Vereinbarung führen würden (z. B. aufgrund der Einführung eines neuen Verarbeitungszwecks), ist eine vorherige Vereinbarung zwischen den Parteien erforderlich.

9.2

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Umsetzung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Die Umsetzung offensichtlich rechtswidriger Weisungen darf der Auftragnehmer ablehnen. Der Auftragnehmer ist nicht verpflichtet, Weisungen des Auftraggebers rechtlich zu überprüfen.

10. Haftung

Es gelten die Regelungen der Leistungsvereinbarung.

11. Löschung und Rückgabe von personenbezogenen Daten

11.1

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.

11.2

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 nach dessen Wahl auszuhändigen/zurückzugeben oder datenschutzgerecht zu vernichten/löschen, soweit er nicht nach geltendem Recht zur weiteren Speicherung verpflichtet ist. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Vernichtung/Löschung ist auf Anforderung vorzulegen.

11.3

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

12. Verschiedenes

12.1

Im Falle eines Widerspruchs haben die Bestimmungen dieser Vereinbarung Vorrang vor den Bestimmungen der Leistungsvereinbarung zwischen dem Auftraggeber und dem Auftragnehmer.

12.2

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam, ungültig oder undurchführbar sein oder werden, so berührt dies nicht die Gültigkeit der übrigen Bedingungen dieses Vertrags.

Ergänzende Vertragsbedingungen zur Auftragsverarbeitung gem. Art. 28 DSGVO

Anlage 1 – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen und Betriebsräumen, Einsatz eines zentralen Zugangsberichtigungssystems über Betriebsausweise, Schlüssel, elektrische Türöffner, 24/7 Wachdienst, Alarmanlagen an der Außenhaut, Videoüberwachungsanlagen, Dokumentation von Besuchern und Ausgabe von Besucherausweisen;
- Zugangskontrolle: Keine unbefugte Systembenutzung, Benutzerrichtlinie für Passwortvergabe, automatische Sperrmechanismen der Systeme, Unterweisung in Sicherheitsrichtlinien;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, Berücksichtigung des Need-To-Know-Prinzips (Datensparsamkeit);
- Trennungskontrolle: Personenbezogene Daten werden streng getrennt voneinander verarbeitet. Bewerber- und Mitarbeiterdaten werden lediglich von HR bearbeitet und fließen in andere Systeme ein als Kunden- und Lieferantendaten.
- Pseudonymisierung: Die Verarbeitung personenbezogener Daten erfolgt wo der Zweck der Verarbeitung es zulässt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;
- Alte Datenträger (Festplatten, Papier) werden von einem Entsorgungsdienstleister vernichtet;

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

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, E-Mail-Verschlüsselung. Virtual Private Networks (VPN) werden zwischen den Standorten geschaltet, SSL-Verschlüsselte Übermittlungen zu Dienstleistern verwendet;
- Es erfolgt grundsätzlich kein physischer Transport personenbezogener Daten;
- Eingabekontrolle: Ein Dokumentenklassifizierungssystem wurde umgesetzt;
- Regelmäßige Datenschutz-Awareness-Trainings für Mitarbeiter und Führungskräfte;

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

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Notfall-Pläne, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, regelmäßige Penetrationstests der Infrastruktur-Sicherheit, Information-Security-Incident-Management;
- Rasche Wiederherstellbarkeit durch hochredundante Speicherung personenbezogener Daten; Einsatz eines zentralen Sicherheits-Patch-Managements.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Konzernweites Datenschutz-Management, definierte Rollen und Verantwortlichkeiten für Datenschutzbeauftragte, Koordinatoren und Verantwortliche;
- Auftragskontrolle: Es erfolgt Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, dies ist sichergestellt durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht und Nachkontrollen.