Annex 4: Auftragsdatenverarbeitungsvertrag

(Version 1.0, 17.10.2024)

zwischen

METEOCONTROL als Auftragsverarbeiter im Sinne der DSGVO

und

KUNDEN als Verantwortlicher im Sinne der DSGVO

1. ALLGEMEINES 2
2. GEGENSTAND DER AVV 2
3. RECHTE UND PFLICHTEN DES KUNDEN 3
4. RECHTE UND PFLICHTEN DER METEOCONTROL 4
5. KONTROLLBEFUGNISSE 6
6. UNTERAUFTRAGSVERHÄLTNISSE 6
7. VERTRAULICHKEITSVERPFLICHTUNG 8
8. WAHRUNG VON BETROFFENENRECHTEN 8
9. GEHEIMHALTUNGSPFLICHTEN 8
10. VERGÜTUNG 9
11. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR DATENSICHERHEIT 9
12. DAUER DER AVV 9
13. BEENDIGUNG 10
14. ZURÜCKBEHALTUNGSRECHT 10
15. SCHLUSSBESTIMMUNGEN 10

ANLAGE 1 DES ANNEX DPA: UNTERAUFTRAGNEHMER 11

ANLAGE 2 DES ANNEX DPA: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN DER METEOCONTROL 12

1. Allgemeines

1.1. Die PARTEIEN haben eine Vereinbarung über die Bereitstellung von Cloud-Diensten geschlossen („VERTRAG“). Nach dem VERTRAG erbringt METEOCONTROL gegenüber dem KUNDEN cloudbasierte SERVICES zur Verarbeitung von Daten einschließlich personenbezogener Daten.

1.2. Diese Auftragsverarbeitungsvereinbarung (nachfolgend AVV) im Sinne des Art. 28 EU-Datenschutzgrundverordnung (DSGVO) regelt die Rechte und Pflichten der PARTEIEN, soweit METEOCONTROL personenbezogene Daten für den KUNDEN verarbeitet.

1.3. Sofern in der AVV der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ im Sinne des Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand der AVV

2.1. Der Auftrag des KUNDEN an die METEOCONTROL umfasst folgende Arbeiten und/oder Leistungen:

2.2. VCOM / mc Assetpilot

2.2.1. Gegenstand gemäß dem aktuell gültigen VERTRAG zwischen dem KUNDEN und METEOCONTROL stellt die entgeltliche Überlassung von technischen Lösungen dar, die es ermöglichen, Messdaten von Energieerzeugungsanlagen und Batterien mit Hilfe von internetgestütztem Monitoring zu verwalten (VCOM) sowie Energieerzeugungsanlagen und Batterien im Rahmen von Berechnungen hinsichtlich ihrer (finanziellen) Leistung zu überwachen und vergleichen (mc Assetpilot). Hierunter fällt die vertragsgemäße Nutzung der Software, der technische Support, Schulungsmaßnahmen und Beratungsdienstleistungen.

2.2.2. Davon umfasst sind alle Änderungen und zusätzlichen Dienstleistungen, die zukünftig in dem VERTRAG Anwendung finden.

2.2.3. Folgende Verarbeitungen im Auftrag führt METEOCONTROL für den KUNGEN durch:

2.2.3.1. Innerhalb der bereitgestellten PLATTFORM erhält METEOCONTROL einen Zugriff über einen User. Der KUNDE hat die Möglichkeit eigene User einzupflegen, indem personenbezogene Daten zur Anlage neuer User erfasst werden. Dies ist erforderlich, um die notwendigen Support- und Dienstleistungsarbeiten ausführen zu können. Insofern hat METEOCONTROL die Möglichkeit zur Dateneinsicht bzw. -änderung im Rahmen der Einrichtung durch den KUNDEN.

2.2.3.2. Hosting: METEOCONTROL speichert die personenbezogenen Daten des KUNDEN auf seinen Systemen, um diese für den KUNDEN vorzuhalten und abrufbar zu machen.

2.2.3.3. Supportdienstleistungen: METEOCONTROL greift im Supportfall u.U. auf die Daten des KUNDEN zu, um Fehleranalyse und Problembehebung durchführen zu können.

2.3. meteocontrol academy

2.3.1. METEOCONTROL stellt seinen KUNDEN eine browserbasierte Lernplattform zur Verfügung,

auf welcher sich der KUNDE registrieren kann. Er sowie seine Beschäftigten erhalten damit Zugang zu Lernvideos und anderen Schulungsinhalten, die METEOCONTROL dort bereitstellt.

2.3.2. Folgende Verarbeitungen im Auftrag führt METEOCONTROL für den KUNGEN durch:

2.3.2.1. Hosting: METEOCONTROL speichert die personenbezogenen Daten des KUNDEN auf seinen Systemen, um diese für den KUNDEN vorzuhalten und abrufbar zu machen und ihm den Zugang zur Lernplattform zu ermöglichen.

2.3.2.2. Supportdienstleistungen: METEOCONTROL greift im Supportfall u.U. auf die Daten des KUNDEN zu, um Fehleranalyse und Problembehebung durchführen zu können.

2.4. Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

2.4.1. Dies betrifft folgende Kategorien inklusive der spezifischen Daten:

2.4.1.1. Stammdaten (Vorname, Nachname, Adressangaben, Kontaktdaten (E-Mailadresse, Telefonnummer)) Berechtigungen, Zugangsdaten. Anlagendaten können gegebenenfalls auch personenbezogen sein.

2.4.1.2. Anwenderbezogene Änderungsprotokolle.

2.4.1.3. Anlagendaten, wenn es sich um Privathaushalte handelt.

2.4.2. Kreis der von der Datenverarbeitung betroffenen Personen:

2.4.2.1. Geschäftspartner/Kunden des KUNDEN

2.4.2.2. Mitarbeiter des KUNDEN

3. Rechte und Pflichten des KUNDEN

3.1. Der KUNDE ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch METEOCONTROL. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem KUNDEN. METEOCONTROL steht nach Ziff. 4 Abs. 6 das Recht zu, den KUNDEN auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen.

3.2. Der KUNDE ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. METEOCONTROL wird dem KUNDEN unverzüglich darüber informieren, wenn betroffene Personen ihre Betroffenenrechte gegenüber METEOCONTROL geltend machen.

3.3. Der KUNDE hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der METEOCONTROL getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Die getroffenen technischen und organisatorischen Maßnahmen können der **Anlage 2 dieses ANNEX DPA** entnommen werden. Der KUNDE wird das Ergebnis in geeigneter Weise dokumentieren.

3.4. Der KUNDE hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber der METEOCONTROL zu erteilen. Weisungen können schriftlich oder per E-Mail oder Fax erfolgen.

3.5. Der KUNDE soll weisungsberechtigte Personen benennen. Für den Fall, dass sich die

weisungsberechtigten Personen beim KUNDEN ändern, wird der KUNDE dies dem METEOCONTROL schriftlich oder in Textform mitteilen.

3.6. Der KUNDE informiert die METEOCONTROL unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch die METEOCONTROL feststellt.

3.7. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der KUNDE für deren Einhaltung verantwortlich.

4. Rechte und Pflichten der METEOCONTROL

4.1. METEOCONTROL verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom KUNDEN erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach dieser AVV und/oder den Weisungen des KUNDEN. Eine hiervon abweichende Verarbeitung von Daten ist der METEOCONTROL untersagt, es sei denn, dass der KUNDE dieser schriftlich zugestimmt hat. Die METEOCONTROL verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

4.2. Bei METEOCONTROL ist als betrieblicher Datenschutzbeauftragter nach Art. 37 DSGVO benannt:

Herr Sven Lenz – Deutsche Datenschutzkanzlei
Telefon: +49 831 930653-00
E-Mail: lenz@deutsche-datenschutzkanzlei.de

Der Fachkundenachweis ist dem KUNDEN auf Verlangen vorzulegen. Ein Wechsel des Datenschutzbeauftragten ist dem KUNDEN unverzüglich mitzuteilen.

Soweit METEOCONTROL keinen Datenschutzbeauftragten benannt hat, hat er dem KUNDEN nachzuweisen, dass er zu einer Benennung gesetzlich nicht verpflichtet ist und dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des KUNDEN gewährleisten

4.3. METEOCONTROL sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

4.4. METEOCONTROL ist verpflichtet, ihr Unternehmen und ihre Betriebsabläufe so zu gestalten, dass die Daten, die sie im Auftrag des KUNDEN verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Die METEOCONTROL wird über relevante Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, den KUNDEN informieren (mind. Textform).

4.5. METEOCONTROL wird den KUNDEN unverzüglich darüber informieren, wenn eine vom

KUNDEN erteilte Weisung nach seiner Auffassung gegen die DSGVO oder andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt. METEOCONTROL ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den KUNDEN bestätigt oder geändert wird. METEOCONTROL ist zur Mitteilung verpflichtet, wenn er einer Verpflichtung zur Verarbeitung der personenbezogenen Daten im Auftrag entgegen den Weisungen des KUNDEN unterliegt.

4.6. METEOCONTROL ist verpflichtet, dem KUNDEN jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des KUNDEN, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Ferner wird METEOCONTROL den KUNDEN unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber METEOCONTROL tätig wird und dies auch eine Kontrolle der Verarbeitung, die METEOCONTROL im Auftrag des KUNDENs erbringt, betreffen kann.

4.7. Für den Fall, dass METEOCONTROL feststellt oder Tatsachen die Annahme begründen, dass von ihm für den KUNDEN verarbeitete personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind (Verletzung des Schutzes der im Auftrag verarbeiteten personenbezogener Daten), hat METEOCONTROL den KUNDEN unverzüglich und vollständig darüber zu informieren. Die Information an den KUNDEN hat die in Art. 33 Abs. 3 DSGVO genannten Inhalte zu enthalten, mindestens jedoch

- Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle
- Darlegung der Art der unrechtmäßigen Kenntniserlangung
- Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung
- welche Maßnahmen durch METEOCONTROL getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

METEOCONTROL ist bekannt, dass für den KUNDEN eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der METEOCONTROL wird den KUNDEN bei entsprechenden Meldepflichten unterstützen.

4.8. METEOCONTROL ist bekannt, dass für den KUNDEN eine Benachrichtigungspflicht nach Art. 34 DSGVO bestehen kann. METEOCONTROL wird den KUNDEN dabei entsprechend unterstützen.

4.9. An der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten durch den KUNDEN hat die METEOCONTROL mitzuwirken. Sie hat dem KUNDEN die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

4.10. METEOCONTROL soll dem KUNDEN die Person(en) benennen, die zum Empfang von Weisungen des KUNDEN berechtigt sind. Weisungsempfangsberechtigte Personen der

METEOCONTROL sind:

- Chengl Liu, Manging Director
- Stijn Stevens, CFO, Managing Director

Für den Fall, dass sich die weisungsempfangsberechtigten Personen bei METEOCONTROL ändern, wird der METEOCONTROL dies dem KUNDEN schriftlich oder in Textform mitteilen.

4.11. METEOCONTROL ist verpflichtet den KUNDEN unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zu unterstützen.

4.12. METEOCONTROL ist verpflichtet dem KUNDEN alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung zu stellen.

5. Kontrollbefugnisse

5.1. Der KUNDE hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den PARTEIEN getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des KUNDEN durch die METEOCONTROL jederzeit im erforderlichen Umfang zu kontrollieren.

5.2. METEOCONTROL ist dem KUNDEN gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne der Ziffer 5.1 erforderlich ist.

5.3. Der KUNDE kann in der Regel nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in den Betriebsstätten der METEOCONTROL vornehmen, soweit nicht eine Kontrolle ohne vorherige Anmeldung erforderlich ist, weil anderenfalls der Kontrollzweck gefährdet wäre. Der KUNDE wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe der METEOCONTROL durch die Kontrollen nicht unverhältnismäßig zu stören. METEOCONTROL ist verpflichtet die Kontrolle zu ermöglichen und aktiv dazu beizutragen. Sie hat das Betreten seiner Räumlichkeiten durch den KUNDEN im Rahmen der Kontrolle zu dulden.

5.4. METEOCONTROL ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem KUNDEN im Sinne des Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den KUNDEN zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der KUNDE ist über entsprechende geplante Maßnahmen vom METEOCONTROL zu informieren.

6. Unterauftragsverhältnisse

6.1. Der KUNDE stimmt der Einschaltung der in **Anlage 2 dieses ANNEX DPA** aufgeführten Subunternehmer für die Erbringung der dort beschriebenen Leistungen zu.

6.2. METEOCONTROL ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit anderen oder weiteren Subunternehmern befugt. Er

setzt den KUNDEN hiervon unverzüglich in Kenntnis.

6.3. Der KUNDE ist damit einverstanden, dass METEOCONTROL zur Erfüllung seiner vertraglich vereinbarten Leistungen VERBUNDENE UNTERNEHMEN von METEOCONTROL zur Leistungserfüllung heranzieht. Die Regelungen gem. Ziffer 6.1 gelten entsprechend

6.4. METEOCONTROL hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen KUNDEN und METEOCONTROL getroffenen Vereinbarungen einhalten kann. METEOCONTROL hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist von METEOCONTROL zu dokumentieren und auf Anfrage dem KUNDEN zu übermitteln. METEOCONTROL ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten im Sinne des Art. 37 DSGVO bestellt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Subunternehmer bestellt ist, hat METEOCONTROL den KUNDEN hierauf hinzuweisen.

6.5. METEOCONTROL hat sicherzustellen, dass die in dieser AVV vereinbarten Regelungen und ggf. ergänzenden Weisungen des KUNDEN auch gegenüber den Subunternehmern gelten. METEOCONTROL hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

6.6. METEOCONTROL hat mit dem Subunternehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Dem KUNDEN ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

6.7. METEOCONTROL ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziffer 5 dieses ANNEX DPA) des KUNDEN und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von KUNDEN und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

6.8. Nicht als Unterauftragsverhältnisse im Sinne der Ziffern 6.1 bis 6.5 sind Dienstleistungen anzusehen, die METEOCONTROL bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die METEOCONTROL für den KUNDEN erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. METEOCONTROL ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Wartungs- und Prüfungsleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den

KUNDEN genutzt werden. Die PARTEIEN sind sich darüber einig, dass vorgenannte Wartungs- und Prüfleistungen eine „Auftragsverarbeitung“ im Sinne des Art. 28 DSGVO darstellen.

7. Vertraulichkeitsverpflichtung

7.1. METEOCONTROL ist bei der Verarbeitung von Daten für den KUNDEN zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. METEOCONTROL verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem KUNDEN obliegen. Der KUNDE ist verpflichtet, der METEOCONTROL etwaige besondere Geheimnisschutzregeln mitzuteilen.

7.2. METEOCONTROL sichert zu, dass ihr die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. METEOCONTROL gewährleistet, dass die sich zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen und dass diese Personen mit den für sie maßgeblichen datenschutzrechtlichen Bestimmungen vertraut sind. Die Verpflichtung der Personen ist dem KUNDEN auf Anfrage nachzuweisen. Sofern METEOCONTROL im Zusammenhang mit Leistungen für den KUNDEN an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis im Sinne des § 3 TDDDG (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz) zu verpflichten.

8. Wahrung von Betroffenenrechten

8.1. Der KUNDE ist für die Wahrung der Betroffenenrechte des Kapitels III der DSGVO allein verantwortlich.

8.2. Angesichts der Art der Verarbeitung wird METEOCONTROL den KUNDEN nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dass der KUNDE seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachkommen kann.

8.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem KUNDEN bei der METEOCONTROL entstehen, bleiben unberührt.

9. Geheimhaltungspflichten

9.1. Beide PARTEIEN verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine PARTEI ist berechtigt, diese

Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

9.2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der PARTEIEN nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

10. Vergütung

10.1. Die Vergütung der METEOCONTROL ist in dem VERTRAG vereinbart.

10.2. Sofern keine Regelung zur Entstehung etwaiger Kosten im Rahmen der Kontrollpflichten besteht und der Aufwand das der METEOCONTROL zuzumutende Maß überschreitet, stellt die METEOCONTROL einen Stundensatz von 150 € netto in Rechnung.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

11.1. METEOCONTROL ist verpflichtet im Rahmen der Verarbeitung im Auftrag alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zu ergreifen. Dies gilt auch für den Fall, dass METEOCONTROL die Durchführung der Verarbeitungen im Auftrag im Rahmen von Remote Work oder Telearbeit gestattet.

11.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 2 dieses ANNEX DPA** beigefügt.

11.3. METEOCONTROL ist verpflichtet, die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit und auf ihre Erforderlichkeit gemäß Art. 32 DSGVO hinzukontrollieren und anzupassen. Zu einer Anpassung der in Anlage 2 aufgeführten technischen und organisatorischen Maßnahmen ist METEOCONTROL verpflichtet. METEOCONTROL ist verpflichtet dem KUDNEN die angepasste und aktualisierte Fassung der technischen und organisatorischen Maßnahmen zeitnah mitzuteilen und ihm diese zur Verfügung zu stellen.

11.4. METEOCONTROL wird dem KUNDEN die von ihm nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung des nach Art. 32 DSGVO und des in dieser AVV geregelten Schutzniveaus in dokumentierter Form und in geeigneter Weise zur Verfügung stellen.

12. Dauer der AVV

12.1. Die Vertragslaufzeit der AVV entspricht der des VERTRAGS.

12.2. Der KUNDE kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der METEOCONTROL gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus dieser AVV vorliegt, METEOCONTROL

eine Weisung des KUNDEN vertragswidrig nicht ausführen kann oder will oder METEOCONTROL den Zutritt des KUNDEN oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

13. Beendigung

13.1. Nach Beendigung der Erbringung der Verarbeitungsleistungen hat METEOCONTROL alle in ihren Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen und personenbezogene Daten enthalten, nach Wahl des KUNDEN zu löschen oder diesem auszuhändigen. METEOCONTROL stellt dabei sicher, dass es durch das Löschen unmöglich gemacht wird, dass die in den zu löschenden Daten enthaltenen personenbezogenen Informationen (weiterhin) mit verhältnismäßigem Aufwand zur Kenntnis genommen oder sonst wie in irgendeiner sinnvollen Art und Weise verarbeitet werden können.

13.2. Diese Verpflichtung gilt auch für etwaige Kopien. Die Datenträger der METEOCONTROL sind danach löschen. Dies betrifft auch etwaige Datensicherungen bei METEOCONTROL. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

13.3. Der KUNDE hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten bei METEOCONTROL zu kontrollieren.

14. Zurückbehaltungsrecht

14.1. Die PARTEIEN sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch die METEOCONTROL im Sinne des § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

15. Schlussbestimmungen

15.1. Sollte das Eigentum des KUNDEN bei der METEOCONTROL durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat METEOCONTROL den KUNDEN unverzüglich zu informieren. METEOCONTROL wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

15.2. Für Nebenabreden ist die Textform erforderlich.

15.3. Sollten einzelne Teile dieser AVV unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen der AVV nicht.

Anlage 1 des ANNEX DPA: Unterauftragnehmer

METEOCONTROL nimmt für die Verarbeitung von Daten im Auftrag des KUNDEN Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten.

Unterauftragnehmer	**Zweck der Verarbeitung**	**Geeignete Garantien, soweit Daten in einem Drittland verarbeitet werden**
meteocontrol Italia s.r.l.	Supportdienstleistungen	EU, AVV vorhanden
meteocontrol France SAS	Supportdienstleistungen	EU, AVV vorhanden
meteocontrol Ibérica SL	Supportdienstleistungen	EU, AVV vorhanden
Raising Power GmbH	Supportdienstleistungen	EU, AVV vorhanden
mc Beteiligungs GmbH	Supportdienstleistungen	EU, AVV vorhanden
meteocontrol Romania SRL.	Supportdienstleistungen	EU, AVV vorhanden
meteocontrol North America Inc.	Supportdienstleistungen	SCC abgeschlossen
meteocontrol Japan Corporation	Supportdienstleistungen	Angemessenheitsbeschluss vorhanden; AVV vorhanden.
meteocontrol Chile SpA	Supportdienstleistungen	SCC abgeschlossen
meteocontrol AMEA DMCC	Supportdienstleistungen	SCC abgeschlossen
meteocontrol Taiwan Inc.	Supportdienstleistungen	SCC abgeschlossen
Functional Software, Inc.	Einsatz des Dienstes Sentry.io zur Überwachung der Datenbankperformance und Fehleranalyse; Speicherung der IP-Adressen im Rahmen der Fehlerübertragung.	SCC (Processor to Processor) wurden abgeschlossen
Eurekos Systems ApS	Bereitstellung Plattform für meteocontrol academy	EU, AVV vorhanden
Infrared Power Techsol Pvt. Ltd.	Bereitstellung Supportdienst-leistungen, nicht-EU-Bereich	SCC, AVV abgeschlossen

Anlage 2 des ANNEX DPA: Technische und organisatorische Maßnahmen der METEOCONTROL

Abschnitt A: Wahrung der Vertraulichkeit personenbezogener Daten (Art. 32 Abs. 1 lit. b) DSGVO)

1. Zutrittskontrolle

1.1. Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

1.2. **Maßnahmen**

- Die Verwaltung befindet sich auf einem öffentlich zugänglichen Grundstück. Das Rechenzentrum für den Betrieb der Clouddienste ist auf einem beschränkt zugänglichen Grundstück.
- Es liegt eine Beschreibung/Dokumentation der gesamten am Standort eingesetzten Zutrittskontrollmaßnahmen vor.
- Es existieren maschinelle Zutrittskontrollen zu den Gebäuden.
- Die Unternehmensserver werden in einem abgeschlossenen und zutrittsgesicherten Raum betrieben.

2. Zugangskontrolle

2.1. Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

2.2. **Maßnahmen**

- Für alle Informationssysteme und Dienste gibt es eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen.
- Das WLAN ist vor unbefugtem Zugang gesichert.
- Es ist sichergestellt, dass nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben.
- Es gibt ein formales Freigabeverfahren, welche Systeme und Applikationen mit personenbezogenen Daten zu durchlaufen haben, bevor diese Netzwerkzugang bekommen dürfen.
- Es ist sichergestellt, dass nur autorisierte Geräte von privaten Personen oder Besuchern logischen Zugang zum Netzwerk der Organisation bekommen.
- Es gibt Maßnahmen zur Identifikation und Authentisierung von externem Wartungspersonal.
- Bei der lokalen Wartung durch Externe ist sichergestellt, dass keine

Ausrüstungsgegenstände den DV-Bereich unkontrolliert verlassen können.

- Es gibt differenzierte und mehrstufige Zugriffsberechtigungen.
- Es gibt eine Firewall-, Network- und Password-policy.
- Es sind wirksame Firewalls und Intrusion Detection Systeme im Einsatz.
- Zentrale Verwaltungssysteme sind nur per VPN erreichbar.
- Netzwerke sind logisch (VLANs) getrennt.

3. Zugriffskontrolle

3.1. Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

3.2. Maßnahmen

- Die Benutzer stellen sicher, dass ihre DV-Ausstattung, falls unbeaufsichtigt, ausreichend geschützt ist.
- Es wird der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms gelebt (Clean Desk Policy).
- Für die Gewährleistung der Datensicherheit und der Zugriffssicherung wird eine spezielle Sicherheitssoftware eingesetzt.
- Es gibt Anweisungen, wie mit nicht mehr benötigten Datenträgern (einschließlich beschriebenem oder bedrucktem Papier) umzugehen ist.
- Die Entsorgung oder Weiterverwendung von Geräten, die mit Speichermedien ausgerüstet sind, ist geregelt.
- Eine Regelung für externen Administrativen Zugriff ist vorhanden.
- Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:
  - Automatische Prüfung der Zugriffsberechtigung mit Hilfe eines Passworts
  - Ausschließliche Menüsteuerung je nach Berechtigung
  - Differenzierte Zugriffsberechtigung auf Anwendungsprogramme
  - Differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen)

4. Trennungskontrolle

4.1. Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

4.2. Maßnahmen

- Personenbezogene Daten auf den Systemen werden logisch voneinander getrennt

(unterschiedliche Datensätze in einer einheitlichen Datenbank werden je nach Zweck markiert (softwareseitige Unterscheidbarkeit)).

- Test- und Produktivumgebung sind getrennte Systeme.

5. Pseudonymisierung

5.1. Eine Pseudonymisierung findet nicht statt

Abschnitt B: Wahrung der Integrität personenbezogener Daten (Art. 32 Abs. 1 lit. b) DSGVO)

6. Weitergabekontrolle

6.1. Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist

6.2. Maßnahmen

- Allen neuen Mitarbeitern werden bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz ausgehändigt.
- Die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, werden durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult.
- Es ist sichergestellt, dass Daten nur an die vom KUNDEN festgelegten oder der Zweckbestimmung nach richtigen Adressaten übermittelt werden.
- Es gibt einen Prozess für ausscheidende, insbesondere gekündigte Mitarbeiter.
- Es gibt ein unternehmensweit gültiges Schema für die Klassifizierung von Daten.
- Es gibt eine Kryptographie-Richtlinie die die Verschlüsselung von Datentransfers regelt.

7. Eingabekontrolle

7.1. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

7.2. Maßnahmen

- Stichprobenartig Kontrollen durch den DSB finden statt (auch hinsichtlich der Einhaltung der Löschungsfristen).
- Die protokollierten Daten sind gegen unbefugte Einsicht oder Manipulation geschützt.
- Es wurde ein IT-Sicherheitsbeauftragter bestellt.

Abschnitt C: Wahrung der Verfügbarkeit personenbezogener Daten (Art. 32 Abs. 1 lit. b) DSGVO)

8. Verfügbarkeitskontrolle

8.1. Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

8.2. **Maßnahmen**

- Die Systeme sind gegen Ausfall abgesichert.
- Es werden regelmäßige Backups durchgeführt.
- Es wird Antivirensoftware eingesetzt.
- Es werden ausreichend dimensionierte USVs eingesetzt.
- In regelmäßigen Abständen wird überprüft, ob die Versorgung mit Datenleitungen, Strom und Klimatisierung noch ausreichend ist.
- Die Versorgungsleitungen verlaufen unterirdisch.
- In den Rechnerräumen befinden sich keine wasserführenden Leitungen.
- Es findet eine ständige Überwachung der Ausgangsspannung(en) statt.
- Es gibt Blitzschutzeinrichtungen.
- Im Serverbereich befinden sich keine brennbaren Gegenstände.
- Ein Frühwarnsystem mit automatischen Brandmeldern ist installiert.
- Es sind ausreichend geeignete Feuerlöscher sowie das richtige Löschmittel im Einsatz und dabei wird auf Einheitlichkeit geachtet. In Teilbereichen werden automatische Löschanlagen eingesetzt.
- Es existiert ein Notfallhandbuch und dieses wird laufend aktualisiert.
- Für den DV-Wiederanlauf gibt es eine schriftliche Unterlage (Zusammensetzung und Aufgaben des Katastrophenstabes).
- Es existiert ein Notfallkonzept für das Netzwerk.
- Die Anforderungen an das Backup sind in einem Backup-Konzept dokumentiert.
- Die Backups sind vor Diebstahl und Zerstörung geschützt.
- Es wurden Prozesse für die Sicherung erstellt und diese in Handlungsanweisungen dokumentiert.
- Ob das Backup brauchbar ist, wird regelmäßig getestet.
- Die Einhaltung der Lufttemperatur wird überwacht.
- Es gibt ein Ausweichrechenzentrum.
- Es gibt externe vom Gesamtsystem unabhängige Monitoringsysteme.
- Es wird auf durchgehende Hardwareredundanz geachtet.

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

9.1. Organisatorische Sicherheitskriterien

9.1.1. Organisatorische Sicherheit beschreibt alle organisatorischen Maßnahmen (Handlungsanweisungen, Vorgehensweisen, etc.) zur Gewährleistung und Verbesserung der Sicherheit.

9.1.2. Maßnahmen

- Ein Datenschutz-Managementsystem (DSMS) ist eingeführt.
- Ein Incident-Response-Management ist eingerichtet.
- Eine regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte werden durchgeführt.
- IT-Sicherheitsaudits werden jährlich durchgeführt.

9.2. Incident-Response-Management

9.2.1. Incidents werden über das Incident-Management (Beschreibung im Leitdokument) behandelt. Abgeleitete Maßnahmen sowie eine Liste aller datenschutzrelevanter Incidents/Vorfälle werden im DSMS integriert nachgehalten.

9.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

9.3.1. Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können. Die Daten der betroffenen Personen werden teilweise verschlüsselt vorgehalten. Änderungen und Anpassungen in Systemen werden dem Datenschutzbeauftragen laut Change-Prozess (im Leitdokument definiert) bekannt gegeben. Eine unregelmäßige Überprüfung ist ebenfalls Teil des PDCA-Überprüfungs-Zyklus des Datenschutzbeauftragten.

9.4. Auftragskontrolle

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

9.4.2. Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf die Wahrung der Vertraulichkeit verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.

9.4.3. Sollte METEOCONTROL bei der Datenverarbeitung Auftragsverarbeiter einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der METEOCONTROL im Sinne der Art. 28 DSGVO und Art 32 Abs. 1 DSGVO.

9.4.4. Voraussetzungen für das Eingehen einer Auftragsverarbeitung ist grundsätzlich eine rechtliche Grundlage. Für einen Vertrag zur Auftragsdatenverarbeitung nach Art. 28 Abs. 3 DSGVO müssen alle geforderten Maßnahmen und Vorgaben eingehalten werden.