Vertrag zur Auftragsverarbeitung „Auftragsverarbeitungsvereinbarung“

zwischen

Nutzer des X-4C Forecasts

(Auftraggeber)

und

Westphalia DataLab GmbH

Regina-Protmann-Str. 16
48159 Münster

(Auftragnehmer)

Der Auftraggeber und der Auftragnehmer werden nachfolgend gemeinsam als „Parteien“ oder einzeln als „Partei“ bezeichnet.

Präambel

Der Auftragnehmer ist mit der Verarbeitung personenbezogener Daten des Auftraggebers oder von angeschlossenen Unternehmen gem. Art. 28 der EU-Datenschutzgrundverordnung (EU-DSGVO) betraut aufgrund des zwischen den Parteien geschlossenen Vertrags über die Nutzung des X-4C Forecasts („Hauptvertrag").

Diese Vereinbarung zur Auftragsverarbeitung gilt für alle bestehenden und künftigen Verträge zwischen den Parteien.

Die rechtliche Grundlage für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten wird durch den vorliegenden Vertrag zur Auftragsverarbeitung dergestalt geschaffen, dass für die Parteien nachfolgende Regelungen gelten.

§ 1
Geltungsbereich

1. Dieser Vertrag zur Auftragsverarbeitung („**Auftragsverarbeitungsvereinbarung**") regelt jeweils die bilateralen rechtlichen Beziehungen zwischen dem Auftraggeber und dem Auftragnehmer.
2. Der Auftraggeber verfügt über ein Weisungsrecht gegenüber dem Auftragnehmer. Eine Weisung („**Weisung**") ist eine Anordnung oder Richtlinie des Auftraggebers an den Auftragnehmer, die den formellen Anforderungen nach § 3 Abs. 2 entspricht. Das Recht, Weisungen zu erteilen, bleibt durch die Auftragsverarbeitungsvereinbarung inhaltlich unberührt.
3. **Rangfolge, „lex posterior".** Soweit nicht anders vereinbart, geht eine Weisung dieser Auftragsverarbeitungsvereinbarung vor; ferner verdrängt die spätere Regelung die zeitlich frühere (so ersetzt bspw. eine jüngere Auftragsverarbeitungsvereinbarung eine ältere Weisung).

§ 2
Umfang

Diese Auftragsverarbeitungsvereinbarung regelt die Verpflichtungen der Parteien in Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer. Gegenstand, Umfang sowie Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer sind in **ANNEX 2** konkret beschrieben.

§ 3
Pflichten des Auftraggebers

1. **Rechtmäßigkeit, Rechte Betroffener.** Der Auftraggeber bleibt verantwortliche Stelle im Sinne des Datenschutzrechts. Für die Beurteilung der Zulässigkeit der Datenverarbeitung

sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Die Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten (Art. 15 ff. EU-DSGVO) der Betroffenen erfolgt ausschließlich und erkennbar im Namen des Auftraggebers.

2. **Form von Weisungen.** Der Auftraggeber erteilt Weisungen, die sich auf Art, Umfang und Verfahren der Datenverarbeitung beziehen. Die Weisung erfolgt zumindest in Textform (E-Mail). Mündlich erteilte Weisungen sind durch den Auftragnehmer unverzüglich in Textform zu bestätigen. Die weisungsberechtigte Person, ebenso wie der Weisungsempfänger sind in **ANNEX 1** genannt.

§ 4
Pflichten des Auftragnehmers

1. **Weisungsgebundenheit, Zweckbindung.** Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich für die im **ANNEX 2** genannten Zwecke und im Rahmen der Auftragsverarbeitungsvereinbarung sowie im Auftrag und gemäß den Weisungen des Auftraggebers. Der Auftragnehmer verwendet die personenbezogenen Daten für keine anderen Zwecke, sofern er hierzu nicht rechtlich verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche(n) Verpflichtung(en) mit, es sei denn, eine solche Mitteilung ist aufgrund wichtiger öffentlicher Interessen verboten. Kopien oder Duplikate personenbezogener 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 benötigt werden. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

2. **Richtlinien, Anweisungen und Betriebsvereinbarungen.** Der Auftragnehmer führt die Datenverarbeitung unter Beachtung der für den Auftragsgegenstand beim Auftraggeber relevanten Richtlinien, Anweisungen und Betriebsvereinbarungen durch, soweit deren Inhalt dem Auftragnehmer bei Vertragsschluss oder nachträglich (etwa durch Weisung) zur Kenntnis gegeben wurde.

3. **Datenschutzbeauftragter.** Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten finden sich in **ANNEX 1.** Änderungen sind dem Auftraggeber schriftlich mitzuteilen.

4. **Prüfungen von Aufsichtsbehörden.** Der Auftragnehmer verpflichtet sich, dem Auftraggeber über Kontrollhandlungen und Maßnahmen der Datenschutzaufsichtsbehörden unverzüglich zu unterrichten, soweit diese mit der Verarbeitung der Daten des Auftraggebers in Zusammenhang stehen. Etwa festgestellte Beanstandungen wird der Auftragnehmer innerhalb angemessener Frist beheben und dies dem Auftraggeber mitteilen.

5. **Keine Verarbeitung in Drittstaaten.** Die Verarbeitung der Daten durch den Auftragnehmer findet grds. ausschließlich auf bzw. aus dem Gebiet der Bundesrepublik Deutschland, eines Mitgliedsstaates der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein sonstiges Land bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers und darf zudem nur erfolgen, wenn die besonderen Voraussetzungen für Datenexporte in Drittländer erfüllt sind. Der Auftragnehmer beachtet in diesem Fall die strengen Vorgaben der Datenübermittlung in Drittstaaten aus Art. 44 DSGVO und schließt entsprechende Vereinbarungen mit Auftragsverarbeitern in diesen Drittstaaten.

6. **Schulungen, Datenschutzgeheimnis.** Der Auftragnehmer hat die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen, auf das Datengeheimnis zu verpflichten und sie über die sich aus dieser Auftragsverarbeitungsvereinbarung ergebenden besonderen Datenschutzpflichten, Zweckbindungen und Weisungen zu belehren. Auf Anforderung wird der Auftragnehmer dies dem Auftraggeber nachweisen.

7. **Überwachung**. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften dieser Auftragsverarbeitungsvereinbarung und der Weisungen des Auftraggebers regelmäßig während der gesamten Vertragslaufzeit. Die Ergebnisse der Kontrollen sind dem Auftraggeber auf Verlangen vorzulegen, soweit diese für die Verarbeitung der Daten des Auftraggebers relevant sind. Die Maßnahmen zur Überwachung sind in einem Datenschutzkonzept beschrieben, das dem Auftraggeber auf Anforderung vorzulegen ist.

8. **Datentrennung.** Die verarbeiteten Daten bleiben von sonstigen Datenbeständen strikt getrennt.

§ 5
Technische und Organisatorische Maßnahmen zur Datensicherheit

1. **Umfang, Dokumentation.** Der Auftragnehmer wird angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Veränderung, Löschung oder Vernichtung sowie unbefugtem Zugriff bzw. unbefugter Offenlegung treffen (Art. 32 EU-DSGVO)). Dabei sind der Stand der Technik, die Durchführungskosten, die Art, der Umfang und die Zwecke der Verarbeitung personenbezogener Daten sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die derzeit vom Auftraggeber konkret getroffenen technischen und organisatorischen Maßnahmen sind in **ANNEX 3** dokumentiert. Diese Maßnahmen unterliegen dem Fortschritt und sind mit dem Stand der Technik weiterzuentwickeln. Insoweit ist es dem Auftragnehmer auch gestattet, seine konkret getroffenen Maßnahmen zu ändern, soweit das vertraglich vereinbarte Schutzniveau hierdurch nicht unterschritten wird. Änderungen an den konkret getroffenen technischen und organisatorischen Maßnahmen sind zu dokumentieren und dem Verantwortlichen regelmäßig mitzuteilen, z.B. durch die regelmäßige Bereitstellung einer aktualisierten Liste konkret getroffener Maßnahmen in **ANNEX 3**. Wesentliche

Änderungen sind schriftlich zu vereinbaren. Die Verarbeitung von Daten in Privatwohnungen ist nicht gestattet.

2. **Nachweis der Einhaltung.** Der Auftragnehmer weist dem Auftraggeber auf Anfrage die tatsächliche Einhaltung der technischen und organisatorischen Maßnahmen nach. Der Nachweis kann durch Vorlage eines aktuellen Testats, durch Vorlage von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder durch Vorlage einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

§ 6
Berichtigung, Sperrung und Löschung von Daten

Auf Aufforderung durch den Auftraggeber oder nach Beendigung der Auftragsverarbeitungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände mit personenbezogenen Daten des Auftraggebers dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung bei sich datenschutzgerecht zu vernichten, soweit gesetzliche Aufbewahrungsfristen nicht entgegenstehen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem Auftraggeber auf Verlangen vorzulegen. Die vollständige Löschung bzw. Herausgabe der Daten an den Auftraggeber ist diesem auf Verlangen mit Datumsangabe schriftlich zu bestätigen. Ist eine Löschung nur mit unverhältnismäßigem Aufwand möglich, können die Parteien eine Sperrung der Daten vereinbaren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

§ 7
Unterauftragsverabeiter

1. **Einwilligungsvorbehalt.** Soweit bei der Verarbeitung personenbezogener Daten des Auftraggebers vom Auftragnehmer Unterauftragsverarbeiter einbezogen werden sollen, bedarf dies der vorherigen Zustimmung des Auftraggebers. Die in ANNEX 1 genannten Unterauftragnehmer gelten als vom Auftraggeber genehmigte Unterauftragsverarbeiter. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

2. **Verträge mit Unterauftragsverarbeiter.** Der Auftragnehmer hat die vertraglichen Vereinbarungen mit Unterauftragsverarbeitern so zu gestalten und auch durchzuführen, dass sie mindestens dasselbe Schutzniveau aufweisen, wie es aufgrund dieser Auftragsverarbeitungsvereinbarung und etwaigen Weisungen zwischen Auftraggeber und Auftragnehmer vereinbart wurde. Auf schriftliche Anforderung des Auftraggebers wird der Auftragnehmer dem Auftraggeber Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis erteilen, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen. Kommerzielle Bedingungen darf der Auftragnehmer dabei schwärzen. Der Auftraggeber ist zur Geheimhaltung der gewonnen Informationen verpflichtet.
3. **Kontrollrechte gegenüber Unterauftragsverarbeitern.** Bei der Unterbeauftragung sind dem Auftraggeber nach Möglichkeit direkte Kontrollrechte beim Unterauftragsverarbeiter einzuräumen, die bestenfalls denjenigen entsprechen, die der Auftraggeber nach dieser Auftragsverarbeitungsvereinbarung gegenüber dem Auftragnehmer hat.

§ 8
Kontrollrechte

1. **Kontrollrechte.** Der Auftraggeber hat das Recht, die Einhaltung der Auftragsverarbeitungsvereinbarung, erteilter Weisungen und der datenschutzrechtlichen Vorschriften durch den Auftragnehmer selbst oder durch einen vom Auftraggeber benannten geeigneten und zur Verschwiegenheit verpflichteten Dritten zu kontrollieren bzw. kontrollieren zu lassen. Gleiche Rechte stehen sowie Angeschlossenen Unternehmen zu (§ 328 BGB), die verantwortliche Stelle sind.
2. **Unterstützungspflicht.** Der Auftragnehmer gewährt dem Auftraggeber bzw. den von diesem benannten Dritten bei den Kontrollen angemessene Unterstützung. Insbesondere gewährt der Auftragnehmer Zugang zu Datenverarbeitungsanlagen, erteilt erforderliche Auskünfte und stellt benötigte Dokumentationen zur Verfügung.
3. **Durchführung.** Kontrollen beim Auftragnehmer und dessen Unterauftragnehmern sind rechtzeitig anzukündigen und dürfen den Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigen.

§ 9
Hinweis- und allgemeine Unterstützungspflichten

1. **Rechtswidrige Weisungen.** Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach Meinung des Auftragnehmers gegen gesetzliche Vorschriften zum Datenschutz verstößt. Die beanstandete Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.
2. **Meldung von Fehlern und Unregelmäßigkeiten.** Der Auftragnehmer hat bei der Feststellung von Fehlern oder Unregelmäßigkeiten der Datenverarbeitung für den Auftraggeber unverzüglich den Auftraggeber zu informieren. Dies gilt insbesondere für Fälle des Bekanntwerdens einer Verletzung der Datensicherheit, die unbeabsichtigter- und/oder unrechtmäßigerweise zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung bzw. unbefugten Zugang zu personenbezogenen Daten führt, die im Auftrag des Auftraggebers im Rahmen dieser Auftragsverarbeitungsvereinbarung verarbeiten werden.
3. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten (Art. 15 ff. EU-DSGVO) sowie den datenschutzrechtlichen Pflichten aus Art. 32 bis 36 EU-DSGVO (Dokumentation der getroffenen technischen und organisatorischen Maßnahmen, Meldung von Datenschutzverletzungen an die Datenschutzaufsicht und ggf. die betroffenen Personen sowie Durchführung von Datenschutz-Folgenabschätzungen / Vorabkonsultationen der Datenschutzaufsicht).

§ 10
Dauer des Auftrags

1. Die Auftragsverarbeitungsvereinbarung beginnt und endet nach den Maßgaben des Hauptvertrags.
2. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn
   - personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder Vergleichsverfahren oder durch sonstige vergleichbare Ereignisse gefährdet sind,
   - der Auftragnehmer gegen gesetzliche oder vertragliche Datenschutzbestimmungen verstößt,
   - der Auftragnehmer eine berechtigte Weisung nicht ausführen will oder kann, oder
   - Aufsichtsbehörden Zweifel an der Rechtmäßigkeit der Auftragsverarbeitung äußern.
3. Die Kündigungserklärung bedarf der Textform (E-Mail).

4. **Fortgeltung.** Soweit der Auftragnehmer über die Laufzeit der Auftragsverarbeitungsvereinbarung personenbezogene Daten des Auftraggebers weiterverarbeitet (z.B. Speicherung aufgrund von Aufbewahrungspflichten), gelten die vertraglichen Vereinbarungen zur Zweckbindung und Einhaltung der technischen und organisatorischen Maßnahmen zur Datensicherheit entsprechend fort.

§ 11
Geheimhaltungspflichten

1. Die Parteien verpflichten sich, alle Informationen und Materialien, die sie im Zusammenhang mit der Durchführung dieser Auftragsvereinbarung in mündlicher, schriftlicher, elektronischer, körperlicher oder anderer Form von der anderen Partei erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung dieser Auftragsverarbeitungsvereinbarung zu verwenden.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne dabei zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 12
Haftung und Schadensersatz

1. Macht ein Betroffener gegenüber einer Partei Schadensersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.
2. Die Parteien haften gegenüber Betroffenen Personen entsprechend der in Art. 82 EU-DSGVO getroffenen Regelungen.
3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadensersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

§ 13
Sonstiges

1. **Maßnahmen Dritter**. Sind personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder Vergleichsverfahren oder durch sonstige vergleichbare Ereignisse gefährdet, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.
2. **Schriftform**. Änderungen der Auftragsverarbeitungsvereinbarung bedürfen der Schriftform. Dieses Formerfordernis gilt auch für die Abbedingung der Formklausel.

3. **Salvatorische Klausel**. Sollten einzelne Teile dieser Auftragsverarbeitungsvereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der Auftragsverarbeitungsvereinbarung im Übrigen nicht.

4. **Anwendbares Recht, Gerichtsstand**. Die Auftragsverarbeitungsvereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN Kaufrechts. Ausschließlicher Gerichtsstand ist derjenige des Auftragnehmers.

5. **Funktionsübertragung und sonstige Datenübermittlung.** Ist der Auftragnehmer in seiner Aufgabenwahrnehmung soweit eigenständig, dass er nicht als Auftragsverarbeiter im Sinn des Art. 28 EU-DSGVO angesehen werden kann (Funktionsübertragung) oder erfolgt die Übermittlung aufgrund berechtigter Interessen der datenempfangenden Stelle, so ist der Datenempfänger (Auftragnehmer) und nicht der Datenübermittler (Auftraggeber) verantwortliche Stelle. In diesem Fall gelten die Bestimmungen dieser Auftragsverarbeitungsvereinbarung ebenfalls, jedoch nur insoweit, als dies angesichts der Eigenverantwortlichkeit angemessen ist. Keine Anwendung finden daher dann die Bestimmungen betreffend der Weisungs- und Kontrollrechte des Auftraggebers gegenüber dem Auftragnehmer. Hierzu gehören insbesondere § 3 und § 8 der Auftragsverarbeitungsvereinbarung. Der Auftraggeber (als Datenübermittler) wird vor der Übermittlung eine angemessene Abwägung zwischen den betroffenen Interessen, nämlich seinem eigenen berechtigten Interesse (Funktionsübertragung) oder dem berechtigten Interesse des Datenempfängers (berechtigte Interessen des Auftragnehmer als datenempfangenden Stelle) sowie dem schutzwürdigen Interesse des Betroffenen am Ausschluss der Datenübermittlung, vornehmen. Der Auftragnehmer verwendet personenbezogene Daten des Auftraggebers ausschließlich für die in **ANNEX 2** genannten Zwecke, unter Einhaltung der vereinbarten technischen und organisatorische Maßnahmen zum Datenschutz und insbesondere unter entsprechender Einhaltung der Pflichten nach § 6, § 7 Abs. 1; § 8 Abs. 1; 0 Abs. 2; dieser Auftragsverarbeitungsvereinbarung. Die Parteien sind sich einig, dass im Fall einer Übermittlung von Daten von Beschäftigten, der Auftraggeber (als Datenübermittler) in vollem Umfang gegenüber dem betroffenen Beschäftigten für die Erfüllung der datenschutzrechtlichen Ansprüche dieses Beschäftigten verpflichtet bleibt.

ANNEX 1

1. Ansprechpartner / Weisungsempfänger beim Auftragnehmer

Name, Vorname oder Zuständigkeit, Funktion	Kontaktdaten
Cornerlius Brosche Gechäftsführer	Westphalia DataLab GmbH Regina-Protmann-Str. 16, 48159 Münster Telefon: +49 (0) 251 20751120 Email. support@westphalia-datalab.com

2. Datenschutzbeauftragter des Auftragnehmers

Name, Vorname oder Zuständigkeit, Funktion	Kontaktdaten
Krecker, Matthias Head of Operations	Westphalia DataLab GmbH Regina-Protmann-Str. 16, 48159 Münster Telefon: 0151 68 969 874 Email: krecker@westphalia-datalab.com

3. Unterauftragsverarbeiter

Name	Kontaktdaten
Amazon Web Services, Inc.	Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States

ANNEX 2

Konkretisierung der Datenverarbeitung

1. Gegenstand der Verarbeitung & Dauer der Auftragsverarbeitung

Gegenstand und Dauer des Auftrags ergibt sich aus dem Hauptvertrag.

2. Zweck der Verarbeitung

Die Tätigkeit des Auftragnehmers dient folgenden vereinbarten Zwecken:

Erstellung von Prognosen auf Basis von Vergangenheitsdaten verschiedener betriebswirtschaftlicher Prozesse und Maschinendaten; Ermittlung von Transaktionsdaten wie Absätze, Warenausgangsdaten, Wareneingangsdaten, Personaleinsatz, Anzahl Servicetickets etc.

3. Kategorien personenbezogener Daten

Folgende Kategorien personenbezogener Daten können Gegenstand des Auftrags sein:

Folgende Datenarten können Gegenstand dieses Auftrags sein:		
☒ Stammdaten (Adressen)	☒ Gesundheitsdaten	☒ Personal- und Identifikationsnummern
☒ Alter	☒ Kreditkartendaten	☒ Reisebuchungs- und Reiseabrechnungsdaten
☒ Arbeitszeitdaten	☒ Kundenverhaltensdaten	☒ Telekommunikations-abrechnungsdaten
☒ Namen	☒ Lohn- und Gehaltsdaten	☒ Telekommunikations-verbindungsdaten

Folgende Datenarten können Gegenstand dieses Auftrags sein:		
☒ Bankverbindung inkl. Zahlungsverkehr	☒ Mitarbeiter-bewertungen	☒ Telefonnummern
☒ Bewerberdaten	☒ Beschäftigte (Qualifikationen)	☒ Vertragsdaten
☒ Hobbys	☒ Nutzerkennungen	☒ Zahlungsdaten
☒ E-Mails	☒ Passwörter	☒ Zugangsdaten
Sonstige: Jegliche Art personenbezogener Daten, die in Textform hochgeladen und verarbeitet werden können.		

4. Kategorien betroffener Personen

Folgende Kategorien betroffener Personen können Gegenstand des Auftrags sein:

- Beschäftigte
- Auszubildende und Praktikanten
- Bewerber
- ehemalige Arbeitnehmer
- freie Mitarbeiter
- Gesellschafter, Organe der Gesellschaft
- Angehörige von Beschäftigten
- Kunden
- Interessenten
- Lieferanten und Dienstleister
- Mieter
- Geschäftspartner
- externe Berater

- Besucher
- Pressevertreter

ANNEX 3

Technische und organisatorische Maßnahmen (TOM)

Westphalia DataLab GmbH

1. Maßnahmen zur Sicherstellung der Vertraulichkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b EU-DSGVO)

a) Zutrittskontrolle

Vorgabe / Anforderung:

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Berechtigungskonzept für den Zutritt zu Räumen und Servern
- Beschränkung der Vergabe von personengebundenen Ausweisen, Schlüsselkarten, etc.
- Digitales Schließsystem gewährleistet die Protokollierung erfolgter Zutritte in den Sicherheitsbereich
- Dokumentation der Vergabe und Rückgabe von Schlüsselkarten, etc.
- Schlüsselregelung
- Manuelles Schließsystem
- System für Zutrittsberechtigungen für Mitarbeiter und Dritte
- Regelmäßige Notwendigkeitsabfrage der Zugangsberechtigung: Im Rahmen personeller Veränderungen im Bereich der IT-Infrastruktur / Administration
- Sorgfältige Auswahl von Hilfspersonal z.B. Reinigungskräften
- Schutz durch Sicherheitsfirmen außerhalb der Geschäftszeiten
- Besucherbuch am Empfang / Besucher tragen sichtbare Besucherausweise / Besucher stets in Begleitung von Mitarbeitern

b) Zugangskontrolle

Vorgabe / Anforderung:

Eine Nutzung der DV-Systeme durch Unbefugte ist zu verhindern.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung und Verwendung von Benutzerprofilen auf Personenebene

- Zuordnung von Benutzerrechten
- Begrenzung der Fehlversuche bei der Anmeldung in Systeme der zentralen Datenhaltung
- Passwortrichtlinie inkl. Mindestlänge, Initialpasswortwechsel, Wechselintervall, Mindestanforderungen an Passwörter
- Authentifikation mit persönlicher Benutzerkennung und Passwort
- Einsatz einer dem Stand der Technik entsprechenden Software-Firewall
- Einsatz einer dem Stand der Technik entsprechenden Anti-Viren-Software
- Automatische Bildschirmsperre
- Zugriff auf die Netzwerkinfrastruktur ist physikalisch abgesichert
- Patch-Management in zentraler Datenhaltung durch Einspielen manueller Updates (Sichtung der Updatelage und Einspielen von Updates in sicherheitsrelevanten Fällen) / zentrales Device-Management für Arbeitsgeräte / Vorgaben zu einsetzbarer/geprüfter Software
- Mobile-Device-Policy: Nutzung von Mobilgeräten auf betriebliches Umfeld beschränkt / Grundsatz der Datenminimierung / Einsatz von Verschlüsselungsmechanismen / zugriff auf zentrale Datensysteme nur über verschlüsselte VPN-Verbindung / Nutzung hardwareverschlüsselter externer Datenträger zum kurzfristigen Datentransport nur durch ausgewählte und geschulte Mitarbeiter gestattet / Gastnetz von Firmennetz abgekapselt

c) Zugriffskontrolle

Vorgabe / Anforderung:

Es ist zu gewährleisten, dass die zur Benutzung eines DV-Systems 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.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines differenzierten Berechtigungskonzepts, Freigabe der Daten nur für Befugte (projektbezogen)
- Verwaltung der Zugriffsrechte durch Administrator
- Anzahl der Personen mit „Administrator-Status“ minimiert
- Externer Zugriff auf das Firmennetz über gesicherte VPN-Verbindung mit 2 Faktoren-Authentifikation
- Authentifizierung durch Benutzername und Passwort
- Protokollierung der Zugriffe
- Teilweise Zwei-Faktoren-Authentifizierung
- Zeitnahe Sperrung der Konten ausgeschiedener Mitarbeiter
- Einsatz von Aktenvernichtern
- Sichere Aufbewahrung von Datenträgern
- Löschung von Datenträgern nach Verwendung
- Regelmäßige Anwendung von Sicherheits-Patches

- 4-Augen-Prinzip
- Funktionstrennung bei Vergabe von Zugangsberechtigungen: Zentrale Vergabe von Zugangsberechtigungen durch Systemadministration (vertreten durch Geschäftsführung)

d) Trennungskontrolle

Vorgabe / Anforderung:

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Mandantenfähigkeit von Systemen und Sandboxing stellen die getrennte Verarbeitung von Daten sicher
- Trennung von Produktiv- und Testsystem
- Rollen- und Berechtigungskonzept
- Nachweislich logische Trennung der Daten der jeweiligen Kunden des (Unter-) Auftraggebers, d. h. Daten verschiedener verantwortlicher Stellen und/oder (Unter-) Auftraggeber sind getrennt zu verarbeiten und gegenseitiger Zugriff ist auszuschließen

2. Maßnahmen zur Sicherstellung der Integrität der Systeme und Dienste (Art. 32 Abs. 1 lit. b EU-DSGVO)

a) Weitergabekontrolle

Vorgabe / Anforderung:

Es ist zu 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.

Vom Auftragnehmer konkret getroffenen Maßnahmen:

- Daten werden nach Projektabschluss gelöscht / darüber hinaus bestehen keine Aufbewahrungspflichten in Bezug auf Projektdaten
- Kommunikation mit On-Premise-Lösungen erfolgt über eine L2TP/IPsec-VPN-Verbindung (OpenVPN)
- Dem Industriestandard entsprechende verschlüsselte Datenübertragungen (SSL)
- Sicherheit auf Servern des Auftraggebers wird durch SSL-Verschlüsselung gewährleistet
- Dateiaustauschordner werden AES-verschlüsselt
- Arbeitsgeräte werden nach dem Verfahren XTS AES-128 verschlüsselt

- Verschlüsselung der Kommunikation mit hausinternen Diensten basiert auf eigens verwalteter Zertifikatsinfrastruktur (X.509 / höchstmögliche noch praktikable Sicherheit für die Verwahrung von CA)
- Pseudonymisierung wird projektabhängig vorgenommen
- Auf Wunsch kann eine Pseudonymisierung durch Drittanbieter vorgenommen werden
- Verschlüsselung von Datenträgern vor Versand
- Sollte eine Verschlüsselung nachweislich nicht möglich sein, muss ein sicheres Alternativverfahren durchgeführt werden (z. B. verschließbare Transportbehälter)
- Zum externen Datenaustausch kann auf Wunsch des Auftraggebers ein Datenträger mit AES-Hardwareverschlüsselung eingesetzt werden.
- Weitergabe von Daten an Dritte ist untersagt
- Dokumentation der Empfänger und ggf. der Zeitspannen von geplanten Überlassungen bzw. vereinbarter Löschfristen
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen beim physischen Transport von Daten
- Sichere Transportbehälter / -verpackungen beim physischen Transport von Daten

b) Eingabekontrolle

Vorgabe / Anforderung:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Richtlinien zu Eingabe und Erfassung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Basis eines detaillierten Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelles Loggen mit Benutzernamen

3. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b und c EU-DSGVO)

a) Verfügbarkeitskontrolle

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines Backup- und Recovery-Konzepts (redundante Datenspeicherung)

- Notfallprozeduren und Test zur Datenwiderherstellung aus Backup
- Aufbewahrung der Datensicherung an einem sicheren Ort
- Einsatz dem Stand der Technik entsprechender Anti-Viren-Software
- Einsatz dem Stand der Technik entsprechender Software-Firewall
- Sicherheitskonzept für Serverräume
- Alarmsystem, Rauchmelder und Feuerlöschgeräte für Serverräume
- Serverräume nicht unter sanitären Anlagen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Belastbarkeit der Systeme wird durch Oversizing gewährleistet

b) Rasche Wiederherstellung

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Manueller Datenträgeraustausch bei zentraler Datenablage im Serverraum
- Arbeitsgeräte durch regelmäßige Backups widerherstellbar

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

a) Auftragskontrolle

Vorgabe / Anforderung:

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Vertragliche Regelung der Zusammenarbeit zwischen Auftraggeber und (Unter-)Auftragnehmer
- Monitoring (Überwachung) der Infrastruktur – eine technische und funktionale Erweiterung wird entsprechend des Weiteren Ausbaus der Infrastruktur vorgenommen
- Auf Wunsch keine Persistierung der Daten außerhalb der Kundenarchitektur
- Sorgfältige Auswahl von Auftragnehmern
- Kontrolle der technischen und organisatorischen Maßnahmen beim (Unter-)Auftragnehmer
- Vereinbarung von Stichprobenkontrollen (z.B. bei Änderungen, turnusmäßig)
- Sicherstellung von Datenrückgabe/-löschung

- IT-Sicherheitskonzept sieht fortlaufende Weiterentwicklung und Anpassung vor. Dabei finden die Konzepte Privacy by Design und Privacy by Default Berücksichtigung (Art. 25 EU-DSGVO).

b) Incident-Response-Management

- Auswertung der Protokollierung (Log-Dateien): Erstellung von verschlüsselt abgelegten Log-Dateien über Zugriffe auf Systeme und Dateien, Änderungen an Ordnern, Rechten und Usern. Logdateien werden durch IT-Administrator/ISB ausgewertet. Auffällige Aktivitäten werden automatisch gemeldet und unterbunden.
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen: Überwachung der zentralen Datenhaltung und der erfolgten Zugriffe auf die Systeme
- Dokumentierter Prozess zum Umgang mit Sicherheitsvorfällen: Interner Prozess zum Umgang mit Datenpannen (Zuständigkeiten/Sofortmaßnahmen/Meldekette)
- Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen

c) Datenschutzrechtliche Voreinstellungen

- Bei jeglichen Analyseansätzen und der Algorithmik werden durch entsprechende Vorauswahl (Feature-Reduction) die Grundsätze von Privacy by Design und Privacy by Default berücksichtigt.

d) Sonstige Überprüfungsmaßnahmen

- Regelmäßige Self-Assessments als Bestandteil eines PDCA-Zyklus