Allgemeine Geschäftsbedingungen Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

für

Claims Information System (CIS)

Präambel

Diese Allgemeinen Geschäftsbedingungen Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO (im Folgenden „AV-Vertrag“ genannt) konkretisieren die Verpflichtungen zum Datenschutz, die sich aus einem vom Auftraggeber genutzten Dienstleistungsvertrag für CIS Information System (CIS) (nachstehend „Vertrag“ oder „Hauptvertrag“ genannt) ergeben.

Der AV-Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen personenbezogene Daten (nachfolgend „Daten“ genannt) durch den Auftragnehmer oder durch den vom Auftragnehmer Beauftragten verarbeitet werden.

Dieser AV-Vertrag trägt Art. 28 Abs. 3 DSGVO (Datenschutzgrundverordnung) Rechnung, nach dem jedes Unternehmen, das Daten im Auftrag verarbeiten lässt, einen Vertrag oder ein anderweitiges Rechtsinstrument nutzen muss, um die Verarbeitung von Daten zu regeln. Es sind speziell Vereinbarungen zu den Verantwortlichkeiten, dem Gegenstand und der Dauer der Verarbeitung, Art und Zweck der Verarbeitung, der Art der verarbeiteten Daten sowie den Rechten und Pflichten der Vertragsparteien zu treffen.

§ 1 Gegenstand und Dauer der Verarbeitung

1. Auftragnehmer ist
   UBIMET GmbH
   Donau-City-Straße 11
   1220 Wien
   Österreich
2. Gegenstand der Vereinbarung sind die Rechte und Pflichten des Auftragnehmers und seiner Kunden (Auftraggeber) im Rahmen der Leistungserbringung gemäß der Leistungsbeschreibung des Hauptvertrags, soweit eine Auftragsverarbeitung von personenbezogenen Daten durch den Auftragnehmer gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer im Rahmen dieser Auftragsverarbeitung, durchführt. Dies gilt auch, sofern der Vertrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.
3. Die Dauer der Verarbeitung richtet sich nach der Dauer und der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung

1. Die Art der Verarbeitung umfasst alle Arten von Verarbeitung im Sinne der DSGVO zur Erfüllung des Hauptvertrags.
2. Zweck der Verarbeitung sind alle, zur Erbringung der im Hauptvertrag vereinbarten Leistungen, insbesondere die Bereitstellung des Claims Information System („CIS“) – ein innovativer Wetterdatenservice für punktgenaue Wetterinformationen zu ausgewählten Wetterereignissen (z.B. Blitz oder Wind/Sturm) für die jüngere Vergangenheit über eine Portallösung und/oder eine Schnittstelle Der Auftraggeber bzw. Mitarbeiter des Auftraggebers können via Portallösung und/oder eine Schnittstelle entsprechende Wetterinformationen abfragen.

§ 3 Art der personenbezogenen Daten und Kategorien von Betroffenen

1. Die Art der personenbezogenen Daten umfasst:
   a. Identifikationscode (z. B. Schadennummer oder Identifikations-Nummer)
   b. Ereignis/Abfrageort (Postleitzahl, Straße, ggf. Hausnummer oder Geokoordinate)
   c. Schadenzeitpunkt (Datum) oder Schadenzeitraum (Datum von/bis)
   d. Schadenart/Wetterereignis
   e. CIS-LogIn-Daten der Mitarbeiter des Auftraggebers

2. Die Kategorien betroffener Personen umfassen
   a. Versicherte Personen/Versicherungsnehmer des Auftraggebers
   b. Mitarbeiter des Datenverantwortlichen

§ 4 Rechte und Pflichten des Auftragnehmers

1. Die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage des Hauptvertrages in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.
2. Der Auftragnehmer erklärt, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
3. Der Auftragnehmer erklärt, dass er geeignete und angemessene Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der **Anlage Technisch Organisatorische Maßnahmen** zu entnehmen).
4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation). Im Falle einer Datenschutzverletzung wird der Auftragnehmer den Auftraggeber unverzüglich ab Kenntnis der Datenschutzverletzung umfassende Informationen über die Datenschutzverletzung zur Verfügung zu stellen, u.a. die Art der Datenschutzverletzung, die Art der betroffenen Geschäftsdaten, die Kategorien und die Anzahl der betroffenen Personen, die Kategorien und die Anzahl der betroffenen Geschäftsdatensätze, die möglichen Folgen der Datenschutzverletzung, die Maßnahmen, die ergriffen oder vorgeschlagen wurden, um die Datenschutzverletzung zu untersuchen und ihre Auswirkungen möglichst gering zu halten.
6. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen personenbezogenen Daten das Recht zur Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Der Auftraggeber wird den Auftragnehmer rechtzeitig über Datum und Uhrzeit der Kontrolle in Kenntnis setzen.
7. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben und/oder in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben. Der Auftragnehmer darf bestimmte personenbezogene Daten anstelle ihrer Löschung speichern, solange und soweit der Auftragnehmer zwingenden gesetzlichen Bestimmungen unterliegt, die ihn zu einer Aufbewahrung verpflichten.
8. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

§ 5 Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten finden ausschließlich im Gebiet der Republik Österreich, in einem Mitgliedstaat 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 Artikel 44 – 50 EU-DSGVO erfüllt sind.

§ 6 Sub-Auftragsverarbeiter

1. Als Sub-Auftragsverarbeiterverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die unmittelbar mit der Erbringung der im Hauptvertrag beschriebenen Dienstleistung in Zusammenhang stehen und durch verbundene oder fremde Unternehmen erbracht werden.
2. Mit dem Hinzuziehen verbundener oder fremder Unternehmen durch den Auftragnehmer ist der Auftraggeber einverstanden. Der Auftragnehmer hat den Auftraggeber von der Beauftragung in Kenntnis zu setzen, sodass dieser innerhalb einer Frist von 14 Tagen widersprechen kann.
3. Eine Liste der aktuell eingesetzten Sub-Auftragsverarbeiter inklusive Tätigkeitsumfang der **Anlage Sub-Auftragsverarbeiter** zu entnehmen.
4. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Der Auftragnehmer behält die volle Verantwortung für die von ihm eingesetzten Sub-Auftragsverarbeiter.

§ 7 Wahrung von Geschäftsgeheimnissen

Die Parteien verpflichten sich zu strikter Vertraulichkeit Dritten gegenüber. Die Parteien sind insbesondere verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekannt werdenden Geschäfts- und Betriebsgeheimnisse, Herstellungsverfahren, Arbeitsmethoden und sonstigen geschäftlichen bzw. betrieblichen Tatsachen, Unterlagen und Informationen der anderen Partei sowie ihrer Kunden und Geschäftspartner streng vertraulich zu behandeln, in keiner Weise Dritten zugänglich zu machen oder sonst zu verwenden, vorbehaltlich anderer vertraglicher Absprachen. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig.

Stand: 21. Dezember 2022

Anlage Technisch Organisatorische Maßnahmen
Technisch-Organisatorische Maßnahmen nach EU-DSGVO/DSG-neu

1. Zugangskontrolle

Definition: Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Kombiniert den Schutz des Gebäudes/Betriebs mit dem Schutz der IT-Systeme.

- Zutritt zum Gebäude: Die Räumlichkeiten des Unternehmens liegen in einem nicht bewohnten Gebäude. Der Zutritt ist nur über ein Schlüssel-Schließsystem möglich.
- Zutritt zu den Büroräumen: Der Zutritt ist nur für die Mitarbeiter über ein Schließsystem möglich. Die Schlüsselübergabe ist in einem Übergabeprotokoll festgehalten
- Besucher: Es ist ein Empfang eingerichtet. Besucher erhalten nur auf Klingeln Einlass und werden grundsätzlich begleitet.
- Serverraum: Der Zutritt zum Serverraum ist nur berechtigen Mitarbeitern gestattet.
- Kommunikationsverbindungen: Diese befinden sich in einem abgeschlossenen Technikraum.
- Zur Sicherung der IT-Systeme werden Firewalls und Virenscanner systemweit eingesetzt und regelmäßig gewartet.
- Für jedes Informationsverarbeitende System sind angemessene Authentifizierungsverfahren festgelegt.
- Passwörter müssen eine Mindestlänge von 8 Zeichen aufweisen und eine Mischung aus Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen enthalten.
- Nicht mehr benötigte Berechtigungen werden zeitnah wieder entzogen.
- 24/7 Sicherheitsdienst im Rechenzentrum, CCTV
- Physische Zugangskontrolle im Rechenzentrum mit Vereinzelungsschleuße

2. Datenträgerkontrolle

Definition: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

- Externe Datenträger und Laptops werden mit einem zeitgemäßen Verfahren wirksam verschlüsselt und dadurch vor dem Zugriff unbefugter Dritter geschützt.
- Mobile Endgeräte verfügen über einen ausreichenden Passwortschutz und sind vollständig verschlüsselt.

- Ein Berechtigungskonzept regelt den Zugriff. Darin sind alle Zugänge differenziert nach Berechtigungsstufen hinterlegt, so dass eine unbefugte Verarbeitung und Nutzung von personenbezogenen Daten nicht möglich ist.
- Mobile Datenträger werden, sofern Sie kritische Daten enthalten, verschlüsselt in einem verschließbaren Schrank aufbewahrt. Sofern sie nicht mehr benötigt werden werden die Daten gelöscht und das Speichermedium mehrfach überschrieben.

3. Speicherkontrolle

Definition: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

- Der Zugang zu Verarbeitungsanlagen für Unbefugte wird verhindert. Dies erfolgt zum einen physisch (Server befinden sich in einem zutrittsgesicherten Raum), zum anderen auf logischer Ebene durch ein Berechtigungskonzept.
- Ein Berechtigungskonzept regelt den Zugriff. Darin sind alle Zugänge differenziert nach Berechtigungsstufen hinterlegt, so dass eine unbefugte Verarbeitung und Nutzung von personenbezogenen Daten nicht möglich ist.
- Berechtigte Benutzer müssen sich identifizieren und authentifizieren.
- Bildschirme werden bei Inaktivität automatisch gesperrt.
- Bei kritischen Systemen ist nach einer zentral festgelegten Zeitspanne einer Leerlaufverbindung eine Reauthentifizierung notwendig.
- Der Login auf Serversysteme wird protokolliert.
- Daten werden verschlüsselt übertragen.

4. Benutzerkontrolle

Definition: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

- Ein Berechtigungskonzept regelt den Zugriff. Darin sind alle Zugänge differenziert nach Berechtigungsstufen hinterlegt, so dass eine unbefugte Verarbeitung und Nutzung von personenbezogenen Daten nicht möglich ist.
- Benutzer müssen sich identifizieren und authentifizieren.
- Datenverarbeitungssysteme sind mit Passwörtern gesichert. Hierfür existiert eine Passwortrichtlinie.
- Daten werden verschlüsselt übertragen.
- Der Zugriff auf alle Anwendungsserver und vertraulichen Informationen ist nur auf geschultes Personal beschränkt.
- Die Zugriffssteuerung wird zentral verwaltet und regelmäßig überprüft.
- Das Prinzip der geringsten Rechte wird angewendet

5. Zugriffskontrolle

Definition: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- Ein Berechtigungskonzept regelt den Zugriff. Darin sind alle Zugänge differenziert nach Berechtigungsstufen hinterlegt, so dass eine unbefugte Verarbeitung und Nutzung von personenbezogenen Daten nicht möglich ist.
- Benutzer müssen sich identifizieren und authentifizieren.
- Zugriffsversuche werden protokolliert.
- Es existiert eine Differenzierung zwischen Rechten zum Lesen und zum Verändern.
- Der Zugriff auf das Verarbeitungssystem erfolgt verschlüsselt.
- Rollenbasiertes Berechtigungskonzept unter dem Prinzip der Geringsten Rechte.

6. Übertragungskontrolle

Definition: Gewährleistung, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Personenbezogene Daten werden entweder über verschlüsselte Verbindungen oder als verschlüsseltes Dokument übertragen.

- Von Heimarbeitsplätzen wird ausschließlich über eine VPN Verbindung.
- Es bestehen Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können.

7. Eingabekontrolle

Definition: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

- Die Eingabe, Änderung und Löschung von Daten wird nachvollziehbar dokumentiert. Dabei werden individuelle Benutzernamen vergeben.
- Ein Berechtigungskonzept regelt die Eingabemöglichkeit. Darin sind alle Zugänge differenziert nach Berechtigungsstufen hinterlegt, so dass eine unbefugte Verarbeitung und Nutzung von personenbezogenen Daten nicht möglich ist.
- Nicht erlaubte Eingaben werden zurückgewiesen.

8. Transportkontrolle

Definition: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

- Datenträger mit personenbezogenen Daten werden ausschließlich von autorisierten Personen verschlüsselt transportiert.
- Eine elektronische Übermittlung erfolgt verschlüsselt.
- Daten werden beim Eingang auf Viren geprüft.
- Nicht mehr benötigte Daten werden umgehend wirksam gelöscht. Der Datenträger wird dabei mehrfach überschrieben.
- E-Mailverkehr wird sofern möglich in bilateraler Abstimmung mit dem Empfänger verschlüsselt. Sollte dies nicht möglich sein werden Dateien mit personenbezogenen Daten mit geeigneten Methoden verschlüsselt.
- Eingehende Datenträger und Daten werden auf Viren überprüft.
- Verschlüsselung aller mobilen Datenträger (Laptop, Smartphones).
- Im Reparaturfall werden kritische Datenträger ausgebaut oder formatiert.

9. Wiederherstellbarkeit

Definition: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Die IT-Systeme sind dokumentiert.
- Es existiert ein Notfallmanagement sowie ein Business Continuity Plan um auf Notfälle entsprechend reagieren
- Das Personal ist bezüglich der Notfallpläne geschult.
- Es existieren für sämtliche kritischen IT-Systeme tägliche Vollbackups. Die eine kurzfristige Wiederherstellbarkeit des jeweiligen Systems gewährleisten. Diese werden in regelmäßigen Abständen auch extern in einem Tresor eingelagert.
- Regelmäßige inkrementelle und volle Backups sowohl auf Storage als auch auf Virtualisierungsebene.

10. Zuverlässigkeit

Definition: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- Die IT-Systeme werden flächendeckend durch eine Monitoringsoftware auf Verfügbarkeit und Funktionsfähigkeit überwacht.
- In regelmäßigen Abständen und beim Bekanntwerden von kritischen Sicherheitslücken werden Sicherheitsupdates durchgeführt.
- Logfiles der Systeme werden aufbewahrt und können ausgewertet werden.

11. Datenintegrität

Definition: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

- Eingaben personenbezogener Daten werden verifiziert.
- Tägliche Backups gewährleisten eine Wiederherstellbarkeit der Daten sofern es zu einer Beschädigung der Daten kommt.
- Storagesysteme sind durch den Einsatz von Raidsystemen ausfallsicher konzipiert.
- In regelmäßigen Abständen bzw. bei Bekanntwerden von Sicherheitslücken werden Sicherheitsupdates der IT-Systeme durchgeführt.
- Ein Mehrschicht-Netzwerksicherheitsschema wird auf alle Dienste angewendet.
- Redundante Firewalls verwalten den Datenverkehr sowohl von außen als auch zwischen den Netzwerkzonen.

- Die folgenden Sicherheitszonen sind definiert
    - Demilitarisierte Zone - DMZ - Dienste, auf die von außen zugegriffen werden muss - wie Load Balancer, FTP-Server, Webserver
    - Externe Zone - Dienste, auf die von der DMZ aus zugegriffen werden kann
    - Interne Zone - Dienste, auf die nur von der externen Zone aus zugegriffen werden kann. Kritische und sensible Informationen dürfen nur in der internen Zone gespeichert werden - also durch mehrere Firewall- und Zugriffsbeschränkungen geschützt werden

12. Auftragskontrolle

Definition: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Hierzu wird auf eine klare Vertragsgestaltung und –ausführung (ADV Verträge) geachtet.
- Auftragnehmer werden sorgfältig im Bezug auch Datenschutz und –sicherheit ausgewählt.
- Die Auftragserteilung wird formalisiert.
- Die ordnungsgemäße Vertragsausführung wird kontrolliert.

13. Verfügbarkeitskontrolle

Definition: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- Es existiert ein Notfallkonzept.
- Es gibt ein Backup und Recovery-Konzept.
- Produktivdaten und Datensicherungen werden an getrennten Orten aufbewahrt.
- Um eine unterbrechungsfreie Stromversorgung zu gewährleisten werden USVs eingesetzt.
- Es existieren Rauchmeldeanlagen.
- Die gesetzlichen Sperr- und Löschfristen werden eingehalten.
- Firewalls schützen die IT-Systeme vor unbefugtem Zugriff von außen.

14. Trennbarkeit

Definition: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene getrennt verarbeitet werden können.

- Ein Berechtigungskonzept regelt den Zugriff. Darin sind alle Zugänge differenziert nach Berechtigungsstufen hinterlegt, so dass eine unbefugte Verarbeitung und Nutzung von personenbezogenen Daten nicht möglich ist.
- Eine logische Mandantentrennung ist gewährleistet.
- Für Entwicklungs- und Testzwecke existieren dedizierte Systeme.
- Besonders sensible Daten werden getrennt von sonstigen Daten gespeichert.

Stand: 21. Dezember 2022

Anlage Sub-Auftragsverarbeiter

Firma, Adresse	Beschreibung Leistung
UBIMET GmbH (Deutschland) Bahnhofplatz 12 76137 Karlsruhe Deutschland	IT-technische Unterstützung/Integrationsprojekte Administration/Vertriebsunterstützung

Stand: 21. Dezember 2022