General Terms and Conditions on Data Processing pursuant to Art. 28 par.3 GDPR

for

Claims Information System (CIS)

Preamble

These General Terms and Conditions on Data Processing pursuant to Art. 28 par 3 of the General Data Protection Regulation (hereinafter referred to as "DP-Contract") specify the data protection obligations arising from a service contract for CIS Information System (CIS) (hereinafter referred to as "Contract" or "Main Contract") used by the customer.

The CP-Contract shall apply to all activities related to the main contract in which personal data (hereinafter referred to as "data") are processed by the contractor or by the contractor's agent.

This CP-Contract takes into account Article 28 (3) of the GDPR (General Data Protection Regulation), according to which any company that has data processed on its behalf must use a contract or other legal instrument to regulate the processing of data. Agreements must be made specifically on the responsibilities, the subject matter and duration of the processing, the type and purpose of the processing, the type of data processed, and the rights and obligations of the contracting parties.

§ 1 Subject and duration of the processing

1. Contractor is
   UBIMET Services GmbH
   Donau-City-Straße 11
   1220 Vienna
   Austria
2. The subject matter of the Agreement is the rights and obligations of the contractor and its customers (client) within the scope of the provision of services in accordance with the service description of the main contract, insofar as a commissioned processing of personal data is carried out by the contractor in accordance with Article 28 of the GDPR. This includes all activities that the contractor performs within the scope of this commissioned processing. This shall also apply insofar as the contract does not expressly refer to this agreement on commissioned processing.
3. The duration of processing depends on the duration and term of the main contract.

§ 2 Type and purpose of processing

1. The type of processing includes all types of processing within the meaning of the GDPR for the performance of the main contract.
2. The purpose of the processing is all, for the performance of the services agreed in the main contract, in particular the provision of the Claims Information System ("CIS") - an innovative weather data service for precisely accurate weather information on selected weather events (e.g. lightning or wind/storm) for the recent past via a portal solution and/or an interface. The customer or the customer´s employees can retrieve relevant weather information via a portal solution and/or an interface.

§ 3 Type of personal data and categories of data subject

1. The type of personal data includes:
   a. Identification code (e.g. claim number or identification number)
   b. Event/location (postal code, street, house number or geo-coordinate, if applicable)
   c. Time of damage (date) or period of damage (date from/to)
   d. Type of damage/weather event
   e. CIS log-in data of the customer's employees.

2. categories of data subjects include
   a. Insured persons/policyholders of the Principal.
   b. Employees of the data controller

§ 4 Rights and obligations of the contractor

1. The processing of the contractual personal data by the contractor shall be carried out exclusively on the basis of the main contract in connection with any instructions by the customer. If the contractor receives an official order to release data of the customer, the contractor shall - to the extent permitted by law - inform the customer thereof without undue delay and refer the authority to the customer.
2. The contractor declares that it has obligated all persons entrusted with the data processing to maintain confidentiality prior to commencement of the activity or that they are subject to an appropriate legal obligation of confidentiality. In particular, the confidentiality obligation of the persons entrusted with the data processing shall remain in force even after termination of their activity and leaving the contractor.
3. The contractor declares that it has taken suitable and appropriate measures to ensure the security of the processing in accordance with Art. 32 of the GDPR (details can be found in the **Annex Technical Organizational Measures**).
4. The contractor shall take the technical and organizational measures to enable the customer to fulfill the rights of the data subject pursuant to chapter III of the GDPR (information, access, correction and deletion, data portability, objection, as well as automated decision-making in individual cases) within the statutory time limits at any time and shall provide the customer with all information necessary for this purpose. If a corresponding request is addressed to the contractor and it is indicated that the applicant mistakenly believes it is the customer of the data processing, the contractor shall immediately forward the request to the customer and inform the applicant thereof.
5. The contractor shall support the customer in complying with the obligations set out in Articles 32 to 36 of the GDPR (data security measures, notifications of personal data breaches to the supervisory authority, notification of the person affected by a personal data breach, data protection impact assessment, prior consultation).
6. The customer shall be granted the right to inspect and control the data processing facilities, including through third parties commissioned by it, with regard to the processing of the personal data provided by it. The contractor undertakes to provide the customer with such information as necessary to control the compliance with the obligations set forth in this agreement. The customer shall inform the contractor in due time about the date and time of the control.
7. After the termination of this agreement, the contractor is obliged to hand over to the customer all processing results and documents containing data and/or to destroy them on the customer's behalf. If the contractor processes the data in a special technical format, it shall be obliged to hand over the data after the termination of this Agreement either in this format or, at the customer's request, in the format in which it received the data from the customer or in another common format. The contractor may store certain personal data instead of deleting it as long as and to the extent that the contractor is subject to mandatory legal provisions that require it to retain it.
8. The contractor shall inform the customer without undue delay if it is of the opinion that an instruction of the customer violates data protection provisions of the Union or the Member States.

§ 5 Place of implementation of data processing

All data processing activities take place exclusively in the territory of the Republic of Austria, in a Member State of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the customer and may only take place if the specific requirements of Articles 44 - 50 EU-DSGVO are met.

§ 6 Subcontracted processor

1. For the purposes of this provision, subcontracted processing relationships shall be understood as those services which are directly related to the provision of the service described in the main contract and which are provided by affiliated or third-party companies.
2. The customer agrees that the contractor consults affiliated or external companies. The contractor shall inform the customer of the assignment so that the customer can object within a period of 14 days.

3. A list of the currently used subcontractors including the scope of activities can be found in the **Annex Sub-contracted Processors**.
4. The contractor shall conclude the necessary agreements within the meaning of Article 28 (4) of the GDPR with the sub-processor. The contractor shall retain full responsibility for the sub-processors used by it.

§ 7 Protection of Business Secrets

The parties undertake to maintain strict confidentiality towards third parties. In particular, the parties are obliged to treat all business and trade secrets, manufacturing processes, working methods and other business or operational facts, documents and information of the other party as well as of its customers and business partners that become known to them on the occasion of the execution of the commission as strictly confidential, not to make them accessible to third parties in any way or to use them in any other way, subject to other contractual agreements. The disclosure of such information is only permitted with the prior written consent of the other party.

Status: 6. January 2023

Annex Technical Organizational Measures
Technical-Organizational Measures according to EU-GDPR/DPR-new

1. Entry control

Definition: Denial of entry to processing facilities with which processing is carried out for unauthorized persons. Combines the protection of the building / operation with the protection of IT systems.

- Access to the building: The premises of the company are located in an uninhabited building. Access is only possible via a key locking system.
- Access to the offices: Access is only possible for employees via a locking system. The key handover is recorded in a handover protocol
- Visitors: There is a reception set up. Visitors will be required to buzz in and are always accompanied.
- Server room: Access to the server room is only permitted for authorized employees.
- Communication connections: These are located in a closed room.
- To secure the IT systems, firewalls and virus scanners are used system-wide and regularly maintained.
- Appropriate authentication procedures are set for each information processing system.
- Passwords must be at least 8 characters long and contain a mix of uppercase and lowercase letters, numbers and special characters.
- Authorizations that are no longer required are revoked.
- The data center is controlled by 24/7 security guards. The premises are under video surveillance (CCTV).
- Access to the data center is controlled via single person access.

2. Data carriers control

Definition: Prevent unauthorized reading, copying, alteration or deletion of data carriers.

- External data storage medium and laptops are effectively encrypted using a state-of-the-art process and thus protected against access by unauthorized third parties.
- Mobile devices have sufficient password protection and are fully encrypted.
- Mobile devices can be remotely deleted in case of loss.
- An authorization concept regulates the access. In it all accesses are differentiated according to authorization levels, so that unauthorized processing and use of personal data is not possible.
- Mobile media, if containing critical data, is stored encrypted in a lockable cabinet. If they are no longer needed, the data is deleted and the storage medium is overwritten several times.

3. Storage control

Definition: Preventing the unauthorized entry of personal data and the unauthorized knowledge, modification and deletion of stored personal data.

- Access to processing facilities for unauthorized persons is prevented. On the one hand, this takes place physically (servers are located in an access-secured room and, on the other hand, on a logical level through an authorization concept.
- An authorization concept regulates the access. In it all accesses are differentiated according to authorization levels, so that unauthorized processing and use of personal data is not possible.
- Authorized users must identify and authenticate.
- Screens are automatically locked when inactive.
- Critical systems require reauthentication after a centrally specified period of idle connection.
- Login to server systems is logged.
- Data is transmitted encrypted.

4. User control

Definition: Prevention of the use of automated processing systems by means of unauthorized data transmission facilities.

- An authorization concept regulates the access. In it all accesses are differentiated according to authorization levels, so that unauthorized processing and use of personal data is not possible.
- Users need to identify and authenticate.
- Data processing systems are secured with passwords. There is a password policy for this.
- Data is transmitted encrypted.
- Access to all application servers and sensitive information is limited to trained personnel only.
- The access control is managed centrally and checked regularly.
- The principle of least rights is applied

5. Access control

Definition: Ensuring that the persons entitled to use an automated processing system have access only to the personal data covered by their access authorization.

- An authorization concept regulates the access. In it all accesses are differentiated according to authorization levels, so that unauthorized processing and use of personal data is not possible.
- Users need to identify and authenticate.
- Access attempts are logged.
- There is a differentiation between rights to read and to change.
- Access to the processing system is encrypted.
- A Role-based authorization concept is used under the principle of least rights.

6. Transmission control

Definition: Ensuring that it is possible to verify and identify where personal data have been transmitted or made available by means of data transmission facilities.

- Personal data is transmitted either via encrypted connections or as an encrypted document.
- Home workstations are only accessed via a VPN connection with authentication.
- It is possible to evaluate the transmission protocols in order to be able to specifically determine the recipients or caller.

7. Input control

Definition: Ensuring that it is possible to retrospectively review and determine which personal data has been entered or changed at any time and by whom in automated processing systems.

- The input, modification and deletion of data is comprehensibly documented. In the process, individual user names are assigned.
- An authorization concept regulates the input option. In it all accesses are differentiated according to authorization levels, so that unauthorized processing and use of personal data is not possible.
- Invalid inputs are rejected.

8. Transport control

Definition: Ensuring that the confidentiality and integrity of the data are protected in the transmission of personal data and in the transport of data media.

- Data carriers containing personal data are transported encrypted only by authorized persons.
- An electronic transmission is encrypted.
- Data is checked for viruses on arrival.
- Data that is no longer required will be deleted immediately. The data carrier is overwritten several times.
- E-mail traffic is encrypted, if possible, in bilateral coordination with the recipient. If this is not possible, files containing personal data will be encrypted using appropriate methods.
- Incoming data carriers and data are checked for viruses.
- Encryption of mobile data carriers as corporate policy (laptop hard drive, smartphone).
- In the case of repair, critical data carriers are removed or formatted.

9. Recoverability

Definition: Ensuring that deployed systems can be restored in the event of a failure.

- The IT systems are documented.
- There is an emergency management and business continuity plan to respond to emergencies
- The staff is trained in emergency plans.
- Daily full backups exist for all critical IT systems. Ensuring the short-term recoverability of each system. These are also stored externally in a vault at regular intervals.
- Regular incremental and full backups on both storage and virtualization levels are implemented.

10. Reliability

Definition: Ensuring that all functions of the system are available and malfunctions are reported.

- The IT systems are monitored comprehensively by a monitoring software for availability and functionality.
- Security updates are made at regular intervals and when critical vulnerabilities become known.
- Logfiles of the systems are stored and can be evaluated.

11. Data Integrity

Definition: Ensuring that stored personal information can not be damaged by malfunction of the system

- Entries of personal data are verified.
- Daily backups ensure data recoverability if data becomes corrupted.
- Storage systems are designed to be fail-safe through the use of RAID systems.
- Security updates of the IT systems are carried out at regular intervals or when security breaches become known.
- A multilayer network security scheme is applied to all services.
- Redundant firewalls manage traffic both from the outside and between the network zones.
- The following security zones are defined
    - Demilitarized Zone - DMZ - services that need to be accessed from outside - such as load balancers, FTP servers, web servers
    - External Zone - Services that can be accessed from the DMZ
    - Internal Zone - services that can only be accessed from the external zone. Critical and sensitive information may only be stored in the internal zone - ie protected by several firewall and access restrictions

12. Processor control

Definition: Ensuring that personal data processed can only be processed in accordance with the instructions of the controller.

- Attention is paid to clear contract design and execution (ADV contracts).
- Processors are carefully selected in terms of privacy and security.
- The instruction of the processors is formalized.
- The orderly execution of the contract is controlled.

13. Availability control

Definition: Ensuring that personal information is protected against destruction or loss.

- There is an emergency concept.
- There is a backup and recovery concept.
- Productive data and backups are kept in separate locations.
- UPSs are used to ensure an uninterruptible power supply.
- There are smoke alarm systems.
- The statutory blocking and deletion periods are adhered to.
- Firewalls protect the IT systems from unauthorized access from the outside.

14. Separability

Definition: Ensuring that personal data collected for different purposes can be processed separately.

- An authorization concept regulates the access. In it all accesses are differentiated according to authorization levels, so that unauthorized processing and use of personal data is not possible.
- Logical client separation is guaranteed.
- Dedicated systems exist for development and testing purposes.
- Particularly sensitive data is stored separately from other data.

Annex Sub-contracted Processors

Firm, Address	Description Service
UBIMET GmbH (Austria) Donau-City-Straße 11 1220 Wien Österreich	identical with services of UBIMET Services GmbH (Austria)
UBIMET GmbH (Germany) Bahnhofplatz 12 76137 Karlsruhe Germany	IT-technical support/integration project administration/sales support

Status: 6. January 2023