General Terms and Conditions

for the usage of the Central & Eastern European Electronic Reporting Information System ("CEERIS") for the usage outside of the scope of River Information Services

(hereinafter also "**T&Cs**")

concluded between

The "**User**" or referred to via their respective role "**Vessel Operator**" or "**Authority**"	and	RGO Communications Ltd, Palinovecka ulica 19/J, HR-10000 Zagreb, Croatia hereinafter the "**Operator**"

"User" and "Operator" are together the "**Parties**"

1. SUBJECT OF THESE TERMS AND CONDITIONS

1.1. These T&Cs regulate the usage of the functions and data provided by the Central & Eastern European Electronic Reporting Information System ("**CEERIS**") for the usage outside of the scope of River Information Services, a web-based tool that processes data in order to provide harmonized information services to support traffic and transport management for inland navigation, including technical interfaces to other modes of transport and electronic reports.

1.2. CEERIS supports Vessel Operators in fulfilling their reporting obligations to the Authorities in an efficient manner and to keep track of which information needs to be sent when to which Authorities. Via CEERIS, Vessel Operators have the possibility to create and forward the required reports (e.g. dangerous goods reports, DAVID forms such as Arrival-/Departure Reports, Passenger Lists, Crew Lists), store them in selected languages and forward them to the Authorities. In this regard, the Vessel Operators will be able to take a number of decisions, including the processing of personal data (e.g. regarding the creation of voyages or deciding which forms and reports, including crew and passenger data, should be sent to which Authorities, etc.).

1.3. Within their respective area of competence, CEERIS also enables the Authorities to create custom views and reports on what forms and information have been sent to them. The Authorities benefit from CEERIS as vessel related data can be easily visualized in different configurations. CEERIS enables Authorities to manage data effectively and transparently and to contact vessel operators in a timely manner.

1.4. The Operator operates CEERIS and provides CEERIS to the Users based on the following T&Cs. Usage of the CEERIS is only possible after acceptance of these T&Cs.

1.5. The CEERIS system administrator monitors the usage of the system and has access to the logfiles and in exceptional cases, in particular for monitoring and bug-fixing, also to the data in order to assure a smooth operation of the CEERIS System.

2. ACCESS AND REGISTRATION

2.1. The User receives access to the system after successful registration, including the creation of a user account. By going through the registration and login process, the User expressly declares to agree to these T&Cs and to comply with them. Further, the User expressly declares that information provided by him is accurate and that he is not impersonating a third party. The User also assures that the person who accepts these T&Cs has obtained the necessary approvals and authorizations to do so on behalf of and with legal effect for the User.

2.2. The access credentials (username and password) which are necessary for the login to CEERIS are confidential and intended exclusively for use by the User. They may not be disclosed to third parties.

2.3. The User is responsible for the security of the user account and is obliged to take appropriate protective measures to prevent unauthorized or unintended access to the user account.

2.4. The User is obliged to immediately report any loss of access data, security concerns, (suspected) security incidents and suspected misuse of his/her account to the Operator.

3. AVAILABILITY AND LIABILITY

3.1. The Operator is not liable for the completeness and the correctness of the entered data as well as for the provision of the forms to the related Authorities as this is the sole responsibility of the Vessel Operator. The Operator is further not responsible and not liable for the acceptance and correct processing of such forms by the related Authorities.

3.2. The Operator will make its best effort to provide uninterrupted access to CEERIS. However, the Operator is not liable for downtimes, interruptions, malfunctions, delays, deletions, changes, incorrect transmissions or memory failures of CEERIS or for incorrect data.

3.3. CEERIS and its use, access, availability, design, features and functions may be discontinued, deactivated, restricted, modified and updated with respect to any User at any time even without prior notice, in particular if this is necessary for legal, technical or operational reasons. This shall not give rise to any rights or claims on the part of the User or third parties.

4. ACCESS TO DATA RELATING TO VESSELS

4.1. The national RIS Providers and/or RIS Authorities serve as Identity Controllers and authenticate requests for becoming a vessel´s data owner in the EuRIS system. The related user data and vessel data is provided to the CEERIS system and thus to the Operator. Access to data relating to vessels will be granted separately by the Identity Controllers. The Operator will make data that can be assigned to individual vessels available to an Authority only, if the Operator is authorized to disclose this data in accordance with the applicable data protection regulations. In particular, the Operator is authorized to do so if the Vessel Operator explicitly grants an Authority access rights as a recipient of this data via the functionalities provided by CEERIS.

4.2. With entering the related data into CEERIS, the User agrees to the storage of the entered data, particularly of personal data (names, IDs, etc. of crew and passengers, etc.).

4.3. Stored data are anonymized and archived after the default storage duration of 30 days or the amended storage duration set by the user. Vessel ID is retained in order to allow for statistical evaluations of reported data for the respective user.

4.4. Based on the information as provided by the Provider according to clause 6.14, the User shall inform the data subjects whose data is processed, on the data processing and obtain the necessary consents (e.g. the Vessel Operator is obliged to comply with EU Data Protection law in relation to the passengers, crew, etc.).

4.5. The Operator does not guarantee to the Authorities that specific data can be provided in relation to a particular vessel.

4.6 At the request of the User, vessel data shall also be shared with Agents which may be involved in the process of checking reporting obligations for the authorities in certain jurisdictions. In such case, these Agents are to be seen as data recipients and the Users shall be obliged to check the admissibility of the respective data transfers and the necessity to conclude contractual agreements with the Agents (if needed) prior to initiating such transfers.

5. DUTIES OF THE USER

5.1. Duties set out in these T&Cs cannot be transferred to third parties.

5.2. Any processing of personal data within the meaning of the EU General Data Protection Regulation 2016/679 (GDPR), including disclosure to third parties, which is not related to the use of CEERIS, is prohibited. This obligation also applies to data generated from CEERIS, which can be allocated to individual vessels.

5.3. The User shall be responsible for creating the technical prerequisites for the unrestricted use of CEERIS. The technical requirements include, in particular, the availability of an up-to-date operating system, uninterrupted Internet access, transmission speed, availability and stability of the network connections and accesses, and the installation of an up-to-date Internet browser (including the corresponding encryption protocol). The costs incurred for these technical prerequisites shall be carried by the User.

5.4. The User agrees to provide, orally or in written form, information about the usage of the CEERIS on request of the Operator.

5.5. The User is obliged to notify the Operator immediately of any interruptions, malfunctions, delays, deletions, changes, faulty transmissions or memory failures in connection with CEERIS, as well as any other defects and problems, and, if necessary, to cooperate appropriately in their rectification.

5.6. CEERIS is not intended to store data permanently. It is the User's responsibility to store data used in connection with CEERIS outside of CEERIS in accordance with the User's requirements and any applicable record retention obligations.

5.7. The User shall be responsible for creating the legal conditions for its use of CEERIS and for complying with all applicable legal provisions (in particular EU data protection and labour law provisions).

5.8. CEERIS is the intellectual property of the RIS Authorities/Providers of the Czech Republic, Austria, Slovakia, Hungary, Croatia, Serbia, Bulgaria and Romania. The User is obliged to refrain from anything that enables him/her or third parties to imitate CEERIS. Furthermore, the User undertakes to use CEERIS only for his own purposes.

6. DUTIES OF THE OPERATOR

6.1. The Operator provides and operates CEERIS. To the extent that personal data are processed in this context, the Operator processes these data on behalf of the respective Users (Controllers) responsible for the vessel-related data as a processor.

6.2. The Operator processes the following data categories for the purpose of operating CEERIS on behalf of the Users and the following categories of data subjects are subject to this processing. The Operator is in particular not responsible for informing the data subjects (e.g. passengers and crew members) about the data processing by CEERIS.

Categories of personal data	Categories of data subjects					
	Vessel Operator and Vessel Owner	Carrier	Crew Members	Passengers	Consignor and Consignee	Agent and other actors in the logistics chain
Position and voyage data including border crossing location and time	x	x	x	x	x	x
Departure data	x	x	x	x	x	x
Destination data	x	x	x	x	x	x
Names	x	x	x	x	x	x
Roles (e.g. crew, passenger, etc.)	x	x	x	x	x	x
Contact information including address	x	x			x	x
Representative	x	x			x	x
Cargo data		x			x	
VAT Number / EORI		x			x	
Identity document data			x	x		
Rank			x			
Sex			x	x		
Date and place of birth			x	x		
Travel document data			x	x		
Visa data			x	x		
Nationality			x	x		
Health status			x	x		
Non-personal data	Not applicable					

6.3. All data processing under these T&Cs is exclusively executed within the territory of the European Union.

6.4. The Operator is entitled to engage the following companies as sub-processors (hereinafter the “Confirmed Sub-Processors”): Amazon Web Services Inc 38, Avenue John F. Kennedy 38, L-1855 LUXEMBOURG, INFINUM d.o.o., Mala Švarča 23, HR- 47000 Karlovac, CROATIA. The Operator must inform the User about intended changes concerning the addition or replacement of the confirmed Sub-Processors. The Operator notifies the User of its intended changes. If the user does not object to the addition or replacement of the confirmed Sub-Processors within two weeks, these changes are considered approved. The Operator enters into a contract with the confirmed Sub-Processors in accordance with Art. 28 para. 4 GDPR. The Operator must ensure that the same data protection obligations as set out in these T&Cs are imposed on the confirmed Sub-Processors. If a confirmed Sub-Processor fails to fulfil its data protection obligations, the Operator remains fully liable vis-a-vis the User for the performance of the confirmed Sub-Processor’s obligations.

6.5. The Operator is obligated to process the data and the processing results exclusively within the scope of the documented instructions of the User, including with regard to transfers of

personal data to a country outside the European Economic Area or an international organization. Should the Operator be required to release data of the User by request of the authorities, then he must – as far as it is legally permitted – inform the User of the above immediately. The processing of data for the Operator's own purposes requires prior written approval by the User.

6.6. The Operator declares legally binding that all persons authorized to process the data have committed themselves to confidentiality, or that they are under an appropriate statutory confidentiality obligation. The confidentiality obligations shall remain in force, even when their authorization to process the data ends and the Operator no longer employs them.

6.7. The Operator declares that he has taken all required measures to ensure the security of the processing in accordance with Art. 32 GDPR. Without limitation to the foregoing, the Operator must implement the technical and organizational measures as outlined in Appendix ./1 as a minimum security standard.

6.8. The Operator must implement appropriate technical and organizational measures so that the User can respond to and comply with requests of data subjects who exercise their rights as data subjects laid down in chap. III of the GDPR (information, access, rectification and erasure, data portability, objection as well as automated individual decision-making) at any time and within the statutory deadlines and the Operator will provide all necessary information to the User. In case the Operator receives a data subject request and if this request shows that the sender of the request mistakenly considers the Operator as User / Controller or if the request relates to CEERIS, then the Operator must immediately forward this request to the User and in alignment with the respective User notify the sender of the request.

6.9. The Operator assists the User in ensuring compliance with the obligations as outlined in Art. 32 to 36 GDPR (data security, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, prior consultation).

6.10. The Operator declares that it maintains a record of processing activities for the data processing under these T&Cs in accordance with Art. 30 GDPR.

6.11. The User is entitled to audit and inspect the data processing facilities of the Operator at any time itself or via a mandated third party (auditor) in order to assess the Operator's compliance with these T&Cs. The Operator is obligated to provide the User with all necessary information and assistance to assess the Operator´s compliance with these T&Cs.

6.12. After the end of the processing under these T&Cs, the Operator is obligated to return to the User or destroy, at the User's request, all data processed on behalf of the User under these T&Cs, including processing results and documents that contain data. Upon request of the User, the Operator must return the data in (i) the unique technical format in which he processes the data for the User, or (ii) in the format in which the Operator received the data from the User, or (iii) in another common format as requested by the User.

6.13. The Operator must inform the User immediately, if he is of the opinion that an instruction of the Controller constitutes a violation of any applicable data protection provisions.

6.14. The Operator provides the Users with data protection information for data subjects under

Art 13 and Art 14 GDPR regarding processing in connection with these T&Cs.

7. DATA TRANSFER TO THIRD COUNTRIES

7.1. The Parties agree to transfer personal data outside of the European Economic Area only if and when the respective User, whose data is exchanged (e.g. the Vessel Operator for vessel related information), has explicitly consented that this data is exchanged. In this connection, the User will also confirm the consent by the data Subjects (e.g. the Vessel Operator regarding the consent of the passengers and the crew). The data exchange consent may be given for a specified duration and may be revoked at any time.

7.2. The Parties agree to conclude the necessary SCCs (e.g. Standard Contractual Clauses between EU and non-EU countries according to Commission Decision 2021/915/EC) if personal data is being transmitted to Users outside of the European Economic Area and if no other legal basis is available (e.g. the decision of the European Commission that a country outside the EU offers an adequate level of data protection). In the event that the SCCs are invalidated, replaced, annulled, or otherwise no longer have the effect of satisfying data transfer restriction obligations under applicable data protection laws, the Parties agree to cooperate in good faith to put in place a replacement data transfer solution that complies with applicable data protection laws. The Appendices of the SCCs (Commission Decision 2021/915/EC) shall be specified in accordance with and by analogous application of these T&Cs and in particular the information contained in clause 6.2.

8. ASSIGNMENTS TO EMPLOYEES AND THIRD PARTIES

8.1. The Parties shall take appropriate measures to ensure data protection, confidentiality and secrecy in the context of the use of CEERIS. In particular, the Parties shall ensure that all obligations of these T&Cs relating to data protection and/or confidentiality and/or confidential treatment of business or trade secrets are transferred to the Parties´ employees and third parties authorized to process the data.

8.2. In the event of a breach of confidentiality by those employees or third parties, the Parties may be held directly liable.

9. DURATION AND END OF THE TERMS AND CONDITIONS

9.1. These T&Cs shall enter into force between a User and the Operator upon acceptance by the User during the login to CEERIS.

9.2. The User has the right to terminate these T&Cs at any time with immediate effect, which results in the deactivation of the CEERIS User account.

9.3. The Operator has the right to terminate these T&Cs at any time with immediate effect, if the Users violate these T&Cs and do not remedy this violation within a period of two weeks after being requested to do so by the Operator. In addition, the Operator has the right to terminate these T&Cs by giving four weeks prior notice effective from the last day of each month.

9.4. Upon termination of these T&Cs, the Parties shall immediately delete all records in such a way that they cannot be recovered and return any documents.

9.5. The following provisions of these T&Cs shall remain in force even after termination / deletion of the user access: 5.8, 6.6, 8 and 11.3

10. CONTACT

10.1. Inquiries, requests, complaints and other type of information (e.g. unauthorized use) shall be submitted to the Operator via e-mail to info@rgo.hr.

11. OTHER CONDITIONS

11.1. These T&Cs as well the acceptance of the User is stored electronically.

11.2. The T&Cs may be amended in specific cases. The amended T&Cs need to be accepted by the User at the first login after the amendment and are hence accepted by the User.

11.3. The related place of jurisdiction for disputes arising out of these T&Cs is exclusively the related court of Vienna. The applicable law is Austrian law. The reference to the provisions of private international law do not apply. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

11.4. If any provision of these T&Cs is or becomes invalid, void or unenforceable in whole or in part, such invalidity, voidness or unenforceability shall not affect the validity, enforceability or enforceability of any remaining provisions. In the event that any of these provisions is or becomes invalid, void or unenforceable, a provision shall be deemed to have been agreed which most closely reflects the intent of the original provision and is not invalid, void or unenforceable.

11.5. The Parties ensure that the person accepting these T&Cs has obtained the necessary internal approvals and has the necessary authorizations and is authorized to accept these T&Cs.

12. APPENDIX ./1 – TECHNICAL-ORGANISATIONAL MEASURES

12.1. Confidentiality

- **Entry control:** Avoidance of unauthorized entry to data processing facilities by: Key, Magnet- or chip cards, electric door opener, doorman, security personnel, alarm system, video system, burglary-restraining windows and/or safety doors, registration at reception desk and identity check, follow-up of visitors on company premises, use of visitor or staff card/ID;
- **Access control**: Avoidance of unauthorized system usage through: Password (including relevant policies), automated locking mechanism, encryption of data carriers, two-factor authentication; Avoidance of unauthorized reading, copying, changing or deleting within the system through: Standard correction profile on a "need to know basis", standard process for assigning authorisations, logging of access, safe storage of data carriers, regular checks of the assigned authorisations and of administrative user accounts in particular, privacy-compliant reuse of data carriers, privacy-compliant disposal of data carriers that are no longer needed, clear-desk/clear-screen policy
- **Pseudonymization**: If possible for the data processing operation, the primary identifiers are removed from within the data processing operation and saved elsewhere.
- **Data classification scheme:** Based on legal obligations or self-assessment (secret/confidential/internal/public).

12.2. Data Integrity[1]

- **Control of data transfer**: No unauthorised reading, copying, changing or deleting during electronic transfer or transport by way of: encryption of data carriers, encryption of data files, virtual private networks (vpn), electronic signatures
- **Data entry control**: Determination of whether and by whom personal data has been entered into the data processing system, changed or deleted by: logging, document management.

12.3. Availability and Resilience

- **Availability control**: Protection against wilful destruction (negligent and/or wilful) or loss through: Back-up strategy (online/offline; on-site/ off-site), uninterrupted power supply (UPS, diesel generator), virus protection, firewall, reporting channels and emergency procedures, security checks with regard to infrastructure and application, multi-level back-up approach with encrypted outsourcing of back-ups in a separated data center, standard procedures for staff changes
- Rapid **recoverability**;
- **Deadline for deletion of data**: Both for data itself and metadata such as log files, etc.

12.4. Procedures for regular testing, assessing and evaluating

- Data protection management, including regular employee training courses;
- Incident-Response-Management;
- Data protection by design;
- **Data processing control:** No data processing in the sense of Art. 28 GDPR without specific instruction by the client through: Definitive contract design, formalized project management, strict selection of data processors (ISO-certified, ISMS), due diligence, follow-up checks.

[1] Prevention of (accidental) destruction, (accidental) damage, (accidental) loss, (accidental) changes of personal data.