

Regulations of the "KZR Module" application (version 1.0) of 17.02.2021.

1. GENERAL PROVISIONS

- 1.1. This document defines the terms and conditions of using the "KZR Module" application, which enables the registered User to fulfil Services within the KZR INiG System.
- 1.2. The administrator of the "KZR Module" internet application is the Oil and Gas Institute – National Research Institute, with its seat in Cracow (31-503), at ul. Lubicz 25 A, NIP (Tax Identification Number): 675-000-12-77
REGON [National Business Registry Number]: 000023136, entered into the Register of Entrepreneurs by the District Court for Cracow-Śródmieście in Cracow, 11th Commercial Division of the National Court Register under number 0000075478.
- 1.3. The Regulations of the application are available at:
http://www.kzr.inig.eu/file/repository/regulamin_aplikacji_KZR.pdf

2. DEFINITIONS

- 2.1. **Application** – the "KZR Module" online application run by the Administrator, enabling the use of the services referred to in the Regulations on the terms specified therein,
- 2.2. **Regulations** – the regulations of the "KZR Module" application,
- 2.3. **User** – a person with an individual account for a specific Application sub-module, designated by the Entity to perform on its behalf activities related to the implementation of the certification process under the KZR INiG System,
- 2.4. **Login** – the User's e-mail address, which is also their individual and unique designation used to use the Application,
- 2.5. **Password** – a sequence of characters selected by the User, which the User uses to secure their access to the Application, meeting the requirements set out in point. 4.24,
- 2.6. **Services** – services provided to the User by the Administrator, available as part of the Application, the type of which is specified in the Regulations,
- 2.7. **The KZR INiG system** (in short: "**System**") – the Certification System for the Sustainable Production of Biofuels and Bioliquids, owned and administered by the Oil and Gas Institute – National Research Institute,
- 2.8. **Administrator** – the Certification System Administrator (in short: "**Administrator**") – a business entity within the meaning of the Act of March 6, 2018 – Business Entity Law, which has the right to use the System. The System Administrator is the Oil and Gas Institute – National Research Institute in Cracow,
- 2.9. **Entity** – Applicant / Participant / Certification Authority,
- 2.10. **Applicant** – means any business entity or natural person participating in the supply chain of biocomponents, liquid biofuels and bioliquids, biomass fuels, recycled carbon fuels, renewable liquid and gaseous transport fuels of non-biological origin, trading unprocessed raw material, processed raw material, fuels, applying for the KZR INiG certificate,
- 2.11. **Participant** – an Applicant who meets the requirements of the System and holds a KZR INiG System certificate, issued by name to that Applicant,
- 2.12. **Certification Authority** (in short: "**Authority**") – a certification body that has been authorized by the Administrator and, acting within the KZR INiG System, has the right to issue a certificate to Applicants / Participants in accordance with the provisions in the System Documents,
- 2.13. **Agreement** – an agreement concluded by the Administrator with the Entity,
- 2.14. **System Documents** – documents regulating the rules of the KZR INiG system, approved by the European Commission in the form of a decision, available at: www.kzr.inig.eu,
- 2.15. **GTC** – "General Terms and Conditions of Agreements concluded with participants and entities applying for certification in the KZR INiG System" regarding agreements with

Applicants and Participants,

- 2.16. **Vulnerability** – a weak spot of an asset or group of assets that can be taken advantage of by at least one threat, understood as a potential cause of an undesirable incident that may lead to damage to the Application,
- 2.17. **Information security event** – the state of the Application, service or network, indicating a possible breach of the Regulations, a security error, or a previously unknown situation that may be related to security,
- 2.18. **Incident** – a single event or a series of undesirable or unexpected events related to information security or reduction of the level of system services, which poses a significant probability of disrupting the operation of the Application and threatens the security of information, including personal data processed in the Application.

3. SCOPE OF SERVICES PROVIDED BY THE ADMINISTRATOR

The scope of services provided by the Administrator includes the operation of the KZR INiG System in accordance with the System Documents and the Agreement, including in particular:

- 3.1. Registration in the KZR INiG System and setting up a User account,
- 3.2. Reporting to the System, in accordance with the requirements specified in the System Documents and GTC,
- 3.3. Using the User's account for the purposes of exchanging and storing correspondence, information and documents with the System, including informing about changes to the System Documents, GTC, Price List and the Regulations.

4. RULES OF USING THE APPLICATION

- 4.1. The Administrator is not responsible for damages arising in connection with the use of the Application, or in connection with the improper operation of the Application due to errors, deficiencies, disruptions, defects, delays in data transmission, computer viruses, failures of the Internet connection or failure to comply with the provisions of the Regulations.
- 4.2. The Administrator is not responsible for the lack of access to the Application for reasons beyond the Administrator's control.
- 4.3. The Application works continuously, and the Administrator warns about the possibility of temporarily suspending the availability of the Application for technical reasons (failure, the need to repair or maintain the systems supporting the Application, and in connection with the need to modernize or extend them, repair or maintain them). In such cases, communication with the Administrator is possible via the following e-mail address: system.kzr@inig.pl.
- 4.4. The Administrator, in connection with the implementation of works regarding the administration or modification of the Application's functionality, for security reasons or other reasons beyond the Administrator's control, has the right to temporarily suspend the Users' access to the Application for the period necessary to perform the planned works or eliminate undesirable events. The Administrator will inform the Users in advance about the planned breaks related to the maintenance works in the Application, by e-mail, to the e-mail address provided for contact.
- 4.5. The User may work in a given session using only one profile – it is forbidden to run several browser sessions at the same time and to work simultaneously in the Application on more than one profile.
- 4.6. For security reasons and for other important reasons beyond the control of the Administrator, the Administrator has the right to temporarily suspend Users' access to the Application for the period necessary to eliminate the consequences of circumstances undesirable for the Administrator.
- 4.7. The Administrator reserves the right to suspend the account of a User who:

- 4.7.1. violates the law or the provisions of the Regulations,
- 4.7.2. takes actions which threaten the security of data collected in the Application,
- 4.7.3. performs illegal activities via the Application,
- 4.7.4. acts to the detriment of the Administrator,
- 4.7.5. provides illegal content,
- 4.7.6. has provided false data in the Application.
- 4.8. The Administrator may permanently block the User's account if the User does not stop acting contrary to the law or the provisions of the Regulations.
- 4.9. The Administrator may delete the User's account if the User has not completed the registration process in the KZR INiG System within 5 months from the date of sending the application.
- 4.10. The Administrator is obliged to send a notification to the relevant Entity about the suspension or blocking of the User's account by e-mail to the e-mail address provided for contact.
- 4.11. In order to use the Application correctly, it is necessary to:
 - 4.11.1. have an Internet connection,
 - 4.11.2. have an installed web browser in the latest stable version (not older than two versions back), e.g., Google Chrome, Mozilla Firefox, Microsoft Edge;
 - 4.11.3. enable Java Script technology, so-called "cookies".
- 4.12. The Administrator collects logs together with the IP addresses from which Users authenticate themselves in the System, solely for the purpose of detecting attempts to breach the System security and for conducting an Application security audit.
- 4.13. By using the Application, the User consents to the Administrator storing on its computer cookies necessary for the proper operation of the Application, which the server can read each time a connection is made from a specific computer. These files are required for the Application to operate, and at the same time do not interfere in any way with the activities and data of the User's computer.
- 4.14. The application uses the following types of cookies:
 - 4.14.1. Session cookie – required for authentication and navigation (switching between application pages), deleted after logging out of the application or after the session expires or after closing the browser;
 - 4.14.2. Security cookie – used to protect against certain attacks, e.g., XSRF (stored and deleted as a session cookie);
 - 4.14.3. User settings cookie (selected interface language, column visibility in lists) – stored until removed from the browser data.
- 4.15. The Application uses only such cookies that are necessary for the proper operation of the Application, and disabling them will prevent logging into the system and performing actions in it.
- 4.16. In order to use the Application, it is necessary to authenticate the User in the Application.
- 4.17. Authentication of the User in the Application takes place using the login and password.
- 4.18. Activation of the account in the Application takes place after clicking the User on the activation link sent in the e-mail to the e-mail address provided by the User during registration.
- 4.19. Upon creating and activating an account in the Application, the User accepts the option of receiving information about the Application by electronic means.
- 4.20. The User is responsible for all activities he/she performs using their login and password.
- 4.21. The User is obliged to read and accept the Regulations, which they confirm (by submitting a declaration on the electronic form) during the first login/registration in the Application.

- 4.22. The submission of the declaration referred to in sec. 4.19 is a prerequisite for accessing the Application. Information about the date and time of the User submitting the declaration is stored in the Application.
- 4.23. Users who have access to the Application are required to comply with the Regulations.
- 4.24. The Application uses passwords configured in accordance with the following security rules:
- 4.24.1. the password consists of a minimum of 8 characters (the maximum password length is 16 characters);
 - 4.24.2. the password consists of uppercase and lowercase letters (minimum one uppercase letter) and numbers (minimum one digit) and special characters (minimum one);
 - 4.24.3. the password is changed least every 90 days;
- 4.25. The duration of an inactive session in the Application (idle time) after which the User automatically logs out is 30 minutes.
- 4.26. In the event of inadvertent disclosure of the password to an unauthorized person or suspected disclosure, the password should be changed to a new one immediately.
- 4.27. If the User cannot change the password (the "Send password" functionality does not work), the Administrator should be notified by email to the following address: system.kzr@inig.pl to change the password.
- 4.28. The password generated by the Application, used by the User to log in for the first time, is provided by e-mail to the User's contact address. The application forces the password change when logging in for the first time. The new password must be different from the previous one.
- 4.29. In order to prevent unauthorized access to the Application, the User:
- 4.29.1. cannot store the login and password for the Application in places accessible to other people;
 - 4.29.2. may not disclose access data to the Application to other persons.
- 4.30. It is forbidden to use the Application with the use of the access data of another User.
- 4.31. The User is obliged to immediately send a notification to the Administrator by e-mail to the following address: system.kzr@inig.pl about a vulnerability, event or incident related to information security.
- 4.32. If the User has problems with accessing the Application, they should contact us by e-mail at the following address: system.kzr@inig.pl.
- 4.33. Any comments and reservations regarding the Application should be submitted by e-mail to the following address: system.kzr@inig.pl.
- 4.34. The rules for concluding and terminating the Agreement with Applicants and Participants under which the Administrator will provide services using the Application, and the conditions for its performance are specified in the GTC.
- 4.35. Agreements with Authorities will be concluded individually in writing (or electronically with a qualified electronic signature). The agreement with the Authority regulates the principles of its amendment and termination as well as the terms of its performance.

5. ADMINISTRATOR'S RESPONSIBILITY

- 5.1. The Administrator undertakes all actions necessary to protect the information and data of the Entity and the User.
- 5.2. The data entered into the Application are collected and processed for the purposes referred to in the Regulations and for the proper functioning of the Application.
- 5.3. The Administrator is not responsible for the content of data entered by the User into the Application.
- 5.4. The User has the right to access the data entered into the Application at any time.
- 5.5. The Administrator takes legally permitted actions to ensure the correct

technical, formal and legal functioning of the Application.

- 5.6. The Administrator is not responsible for any damages resulting from the inability to use or from a malfunction of the Application and improper use of the Application by the User.
- 5.7. The Administrator is not responsible for any resulting damage from the improper operation of the User's computer hardware and software.
- 5.8. The Administrator is not liable for damages caused by the disclosure of the Password by the User to a third party or other actions of the User not in accordance with the Regulations.
- 5.9. The Administrator of the Application is not responsible for damage caused by an external event that is impossible to predict or prevent.
- 5.10. The Administrator's liability towards the User and the Entity for making the Application available to them for use is in each case limited only to damages caused by the Administrator intentionally or resulting from its gross negligence (subject to sections 5.3.–5.9 above).

6. THE PROCESSING OF PERSONAL DATA

- 6.1. The data Administrator is the Oil and Gas Institute – National Research Institute with its seat in Cracow, ul. Lubicz 25 A, 31-503 Cracow, Tel. +48 12 421 00 33, fax: +48 12 430 38 85, email: office@inig.pl.
- 6.2. You can contact the data protection officer in all matters relating to the processing of personal data and the exercise of rights related to data processing by e-mail daneosobowe@inig.pl or in writing to the address of the Administrator's seat.
- 6.3. Personal data will be processed for:
 - in the case of natural persons or natural persons running a sole proprietorship:*
 - 6.3.1. the performance of the Agreement or to take action before its conclusion (Article 6 (1) (b) of the GDPR),
 - 6.3.2. the fulfilment of the legal obligation that is imposed on the Administrator, including: related to archiving, accounting and tax settlements, handling the complaint process, detecting and preventing fraud, other legal obligations imposed on the Administrator (Article 6 (1) (c) of the GDPR) ,
 - 6.3.3. legitimate interests of the Administrator, including: verification of compliance with the requirements in force in the System, conclusion, performance and monitoring of the implementation of the Agreement to which the Entity is a party, ongoing contact and cooperation related to the Agreement, establishing, investigating or defending against claims, contact with the Certification Authority (Article 6 (1) (f) of the GDPR);
 - in the case of persons representing Entities other than a natural person / natural person conducting a sole proprietorship or being their employees:*
 - 6.3.1. the fulfilment of the legal obligation that is imposed on the Administrator, including: related to archiving, accounting and tax settlements, handling the complaint process, detecting and preventing fraud, other legal obligations imposed on the Administrator (Article 6 (1) (c) of the GDPR) ,
 - 6.3.2. legitimate interests of the Administrator, including: the conclusion, performance and monitoring of the implementation of the Agreement to which the Entity is a party, identification of persons authorized to represent the entity, regular contact and cooperation between the Entities related to the Agreement being implemented, establishing, investigating or defending against claims (Article 6 sec. 1 (f) of the GDPR).
- 6.4. The recipients of personal data may be the National Agricultural Support Center, die Bundesanstalt für Landwirtschaft und Ernährung (BLE), the European Commission, Authorities recognized by the Administrator, entities processing personal data on behalf of the Administrator (e.g. entities operating IT systems), other authorities based on 0 legal provisions, as well as other personal data administrators processing data on their own

- behalf, e.g. entities operating by post or courier.
- 6.5. Personal data will not be transferred to third countries or international organizations.
 - 6.6. The data identifying the Entity defined in the System Documents within the KZR INiG system are published at www.kzr.inig.eu.
 - 6.7. Personal data will be stored for 5 years from the end of the Agreement, as well as after its termination, for the time related to the expiry of claims connected to the contract, for the time specified by tax regulations and financial reporting regulations, and then, as far as archival materials are concerned, for the time resulting from provisions of the Act of July 14, 1983 on the national archival resources (consolidated text: Journal of Laws 2020, item 164 as amended). The information in the system logs is stored from the date of their recording for a period of two years, unless detailed regulations specify otherwise.
 - 6.8. The person whose data is processed has the right to access the data (Article 15 of the GDPR), the right to request their rectification (Article 16 of the GDPR), the right to delete it in a situation where data processing does not take place in order to fulfil an obligation arising from a legal provision or in the exercise of public authority (Article 17 of the GDPR), the right to limit processing, and separate provisions may exclude the possibility of exercising this right (Article 18 (1) of the GDPR), the right to object to processing (Article 21 (1) of the GDPR).
 - 6.9. The data subject has the right to lodge a complaint with the supervisory body dealing with the protection of personal data in the Member State of his/her habitual residence, place of work, or place of the alleged infringement. In Poland, such authority is the Office for Personal Data Protection, ul. Stawki 2, 00-193 Warsaw.
 - 6.10. Providing personal data is voluntary, but necessary for the conclusion/performance of the agreement. The consequence of not providing data is the inability to participate in the certification process in the System.
 - 6.11. Personal data is not subject to automated decision making, including profiling.

7. COMPLAINTS

- 7.1. The entity has the right to submit a complaint regarding the operation of the Application to the Administrator to the e-mail address: system.kzr@inig.pl or by post to the address of the Administrator's seat. The Administrator will consider the complaint within 30 days and inform the Entity about the method of settling the matter.

8. FINAL PROVISIONS

- 8.1. Information about changes to the Regulations will be provided to the Entity by electronic means to the e-mail address provided by the Contact Entity and published on the Administrator's website (www.kzr.inig.eu). The Administrator, together with the information about the change, will send the Entity the current text of the document and inform it about the date of entry into force of the planned changes. The date of entry into force of the planned changes may not be shorter than 14 days from the date of providing information about the change to the Entity.
- 8.2. In the period before the effective date of the changes introduced in the Regulations, the Entity may object to the introduced changes. The effects of the objection are specified in the Agreement for the Authorities, and in the case of Applicants and Participants – the GTC. The statement on the objection must be made in writing, otherwise null and void. If, in the period before the date of entry into force of the changes introduced in the Regulations, the Entity does not object to the Administrator against these changes, it is assumed that the Entity has accepted them.
- 8.3. In matters not covered by the Regulations, the GTC and System Documents and GTC apply – in the case of Applicants and Participants, or the Agreement document – in the case of Authorities. In matters not covered by the Regulations, GTC or the Agreement document and System Documents, the provisions of generally applicable Polish law shall apply.