

RULES OF ACCESS TO THE IT SYSTEMS OF KRAJOWY DEPOZYT PAPIERÓW WARTOŚCIOWYCH**Chapter 1****General****§ 1**

1. The Rules of access to the KDPW IT systems, hereinafter the “Rules”, describe the rules of opening access accounts, authenticating of access accounts and the rules of obtaining access to the KDPW applications made available on the Services Portal: <https://online.kdpw.pl>.
2. These rules apply in legal relations arising from agreements concluded by KDPW with participants or other entities which receive services provided by KDPW and functionalities that are available via KDPW’s IT systems to the extent set out in the KDPW regulations concerning such services or functionalities.

§ 2

Whenever the following terms are used in these rules:

- 1) KDPW application – this shall be understood to mean any application used for electronic communication with KDPW as part of a specific service, enabling the exchange of messages between a participant and KDPW using data transmission, available via a dedicated access point;
- 2) Services Portal – this shall be understood to mean the services portal available at <https://online.kdpw.pl>;
- 3) access point – this shall be understood to mean the URL address redirecting to a KDPW application via the U2A interface;
- 3a) U2A interface – this shall be understood to mean a graphical user interface supporting manual exchange of data with KDPW;
- 4) service – this shall be understood to mean a service provided by KDPW or functionalities available to participants via a KDPW application;
- 5) participant – this shall be understood to mean an entity which is a party to a participation agreement concluded under the service rules or a party to another agreement concluded in accordance with the service rules or an entity which gains access to functionalities provided by KDPW via a KDPW application;
- 5a) service group - this shall be understood to mean a list of applications within the Services Portal assigned by KDPW to the participant type indicated in the service regulations, to which access is granted by the rights administrator appointed by the participant;
- 6) service rules – this shall be understood to mean a template agreement which defines the legal relationship between KDPW and a participant, applicable to a service, or another agreement concluded between KDPW and a participant concerning the provision of a service;
- 7) message – this shall be understood to mean information or a declaration which, under the service rules, in relations between a participant and KDPW, may or should be transmitted via means of electronic communication;
- 8) electronic communication – this shall be understood to mean the submission and receipt of declarations of intent and information which, under the service rules, in relations between a

participant and KDPW, may or should be transmitted by or to the participant via a KDPW application;

- 9) KDPW – this shall be understood to mean the company Krajowy Depozyt Papierów Wartościowych S.A.;
- 10) KDPW_CCP – this shall be understood to mean KDPW's subsidiary, KDPW_CCP S.A.

§ 3

1. Electronic communication with KDPW using the U2A interface is available through:
 - 1) the interface used to upload data, or
 - 2) the transmission of structured messages to dedicated message queues.
2. Electronic communication with KDPW using the U2A interface shall only be possible in instances where permitted by the rules of the specific service.
3. Messages provided by a participant to KDPW via the U2A graphical user interface shall be deemed delivered upon the receipt of the message by KDPW, where the receipt of the message shall be defined from the moment when it is saved in the relevant KDPW application. Messages sent by KDPW to a participant via the U2A graphical user interface shall be deemed delivered upon the posting of the message in the application or, depending on the terms of the specific service, upon the dispatch by KDPW to the participant of an email notification of the posting of the message in the application. The email address for the delivery of notifications shall be the address provided in the form referred to in § 7 subpara. 3 point 1 as the address for correspondence. This address shall be confirmed by the participant by submitting a declaration on granting the person referred to in § 7 subpara. 7 point 1 of the authorisation to act on the participant's behalf and, if access is granted by a person authorised by the participant as referred to in § 7 subpara. 7 point 2, it shall be confirmed by that person by granting access to the application.
4. Messages sent to KDPW via the U2A interface using structured messages to dedicated message queues, shall be deemed to have been delivered upon the receipt of the message by KDPW; the receipt of the message shall be the moment the message is subject to validation in the KDPW application. Messages sent by KDPW to a participant shall be deemed to have been delivered upon their entry in the participant's output queue.
5. The communication rules adopted for a given service may create additional obligations for the participant related to the transmission of messages, in particular they may require verification of the identity of the person transmitting the message or appending an electronic signature to the message.
6. KDPW and participants acknowledge the effectiveness of the delivery of messages, subject to the conditions provided for in these rules, and agree that any evidence of such actions may be taken.

§ 4

1. Subject to subpara. 2 to 3, electronic communication with KDPW shall be available to participants on a 24/7 basis.
2. KDPW may make a technical interruption in the operation of a KDPW application in accordance with the rules set out in the service rules or the communication rules adopted for the service.
3. KDPW may make a technical interruption in the operation of the communication interfaces.

Chapter 2

Electronic communication via U2A

Section 1

Opening access accounts

§ 5

1. Electronic communication with KDPW via U2A requires an access account to be opened on the KDPW website.
2. An access account is opened by a natural person acting on his or her own behalf by completing a dedicated form with such person's data required in the form. When completing the form, such person shall make a statement to the effect that he or she gives his or her consent for KDPW to process his or her personal data contained in the form. Failure to give such consent shall prevent the opening of an access account and the submission of an application for access to the KDPW application; withdrawal of the consent shall result in the access account being closed and in the loss of all granted access to KDPW applications. An access account may be opened following the verification of the email address provided in the form by entering in the form a verification code generated by the application and sent to such address.
3. The email address provided in the form shall be the access account identifier (login). The login is not subject to change. In case of a change of email address, the natural person should open a new account and get access to the KDPW application again.
4. Details of how to open and use an access account are available in the account user manual published on the KDPW website.
5. Participants shall immediately report to KDPW any suspected unauthorised use of the access account of a person who gains access to the KDPW application on their behalf.
6. KDPW shall block an access account if the maintenance of the account poses a threat to the security of KDPW's IT systems.
7. KDPW may check activity in access accounts by reviewing access of holders of access accounts to the email addresses used as account identifiers. If KDPW cannot confirm that an account is active, KDPW may block or delete the account and revoke access to the KDPW application of the person who provided the address in the form.

Section 2

Authentication to access accounts

§ 6

1. Logging in to the KDPW application shall require an authentication process for the access account. Authentication is understood to be a process of confirmation by the holder of an access account of the identity the holder declared when opening that account.
2. The basic access account authentication mechanism required for logging into all KDPW applications shall be the login and the access account password defined by the account holder.
3. Logging into KDPW applications available on the Service Portal shall require the use of an additional authentication factor, which is the confirmation of the declared identity using the dedicated mobile application KDPW Group Authenticator.
4. Confirmation using the KDPW Group Authenticator mobile application shall be required for each subsequent login to the Services Portal.
5. The confirmation referred to in subpara. 4 shall not be required when logging in on a computer or mobile device using a browser which has been registered as trusted by the account holder. The account holder may manage browsers marked as trusted using the application available at <https://identity.kdpw.pl>.
6. Authentication to access accounts using the additional authentication factor referred to in subpara. 3 shall allow the account holder to access all KDPW applications to which the holder has been granted access, as well as KDPW_CCP applications available on the Services Portal, in accordance with separate regulations adopted by that company. In the event that the account holder logs in to the KDPW applications through an access point for which only the confirmation with the basic authentication factor is required, logging in to the Services Portal shall require re-authentication to the access account.
7. KDPW shall define the technical requirements for mobile devices on which the KDPW Group Authenticator application can be run. Participants shall provide the person referred to in § 7 subpara. 7 with access to a device that meets these requirements.
8. KDPW shall charge no fee for downloading and using the KDPW Group Authenticator application.
9. Detailed information regarding the download and use of the KDPW Group Authenticator mobile application, including the technical requirements for the mobile devices on which the application can be run, and the rules for managing browsers marked as trusted, are available in the account user manual on the KDPW website.

Section 3

Getting access to KDPW applications available on the Services Portal

§ 7

1. A person holding an access account gains access to the KDPW application based on a request.
2. Access to a KDPW application may require additional data identifying the person authorised by the participant which shall be: PESEL number in the case of persons with Polish citizenship, or date of birth in the case of persons with citizenship other than Polish.
3. A request is submitted as follows:
 - 1) the person authorised by the participant shall complete a dedicated online form available on the Services Portal; and
 - 2) the participant shall deliver to KDPW a statement authorising such person to act on its behalf to the extent defined in the statement and confirming the personal data of the person provided by such person in the form referred to in point 1. Delivery of the statement to KDPW shall not be required where access is granted by the person authorised by the participant referred to in subpara. 7 point 2, or in § 11a; by granting access to the application, that person shall at the same time confirm the personal data of the proxy appointed by them.
4. The statement referred to in subpara. 2 point 2 shall be provided by the participant to KDPW in writing or electronically (in the form of a document bearing a qualified electronic signature). The statement may be delivered in the form of a scan not bearing a qualified electronic signature in the case of a service for which such a form of statement has been indicated as acceptable to a person authorised by the participant in an email message generated automatically after that person has filled in the form referred to in subpara. 3 point 1.
5. Access to a KDPW application may also be granted, if so allowed by the relevant service rules, on the basis of access permissions previously obtained by such person, in particular by granting access to a KDPW application automatically to a person already authorised to access another application.
6. The request referred to in subpara. 3 shall be presented no later than 5 business days before the date when the person authorised by the participant wishes for the first time to send or receive a message via a KDPW application.
7. Unless the service rules provide otherwise, a request may concern the permission for the person authorised by the participant to:
 - 1) communicate electronically with KDPW on behalf of the participant and, if the participant uses the service on behalf of another entity or entities, also to communicate electronically with KDPW on behalf of such entities (user role); or
 - 2) grant to other persons who complete the form referred to in subpara. 3 point 1 for access to the KDPW application to the extent defined in point 1, the authorisation to communicate electronically with KDPW on behalf of the participant and to revoke such authorisation by granting or revoking, respectively, their access to the KDPW application and, if the participant uses the service on behalf of another entity or entities, also to do those things on behalf of such entities (service administrator role).
8. Subject to § 8, KDPW shall accept or reject requests following their formal and content checks.
9. KDPW may automatically remove from the Services Portal a form referred to in subpara. 3 point 1 after a time limit which shall be no less than 90 calendar days after the completion of the form if

the request for access to a KDPW application by the person who filled in the form is not approved by KDPW within such time limit.

10. If a request is rejected or a form is removed, a new request must be filed to gain access to the KDPW application.

§ 8

Taking into account the provisions of § 11a, the terms and conditions of communication defined for a service may provide that KDPW shall accept or reject only requests concerning permissions referred to in § 7 subpara. 7 point 2 (service administrator role). In that case, participants shall authorise at least one person to act on their behalf as service administrator. Access to a KDPW application may be granted or revoked for a person acting on behalf of a participant as user only by the person acting on behalf of the participant who has access to the application as service administrator.

§ 9

1. The list of KDPW applications available to each access account holder on the Services Portal shall be updated upon each login.
2. If access to a KDPW application is granted during the account holder's active session, such access may be used after logging out of the session and logging in once again.
3. An account holder's access to a KDPW application shall be verified during an access session. Failure to confirm access shall result in revocation of access.

§ 10

1. Persons granted access to a KDPW application as users in connection with the participant's presentation of the statement referred to in § 7 subpara. 3 point 2 or an authorisation granted to them under § 7 subpara. 7 point 2 or § 11a shall be deemed authorised by the user to communicate electronically with KDPW via the application and actions of such persons shall be deemed actions of the participant on behalf of the participant or on behalf of an entity represented in the application by the participant. The preceding sentence shall apply also where the form or certificate referred to in § 7 subpara. 3 contains incorrect personal data of the person concerned.
2. Persons granted access to a KDPW application as service administrator in connection with the participant's presentation of the statement referred to in § 7 subpara. 3 point 2 shall be deemed authorised to authorise other persons to communicate electronically with KDPW via the application for the participant on behalf of the participant or on behalf of an entity represented in the application by the participant. The provisions of the second sentence of subpara. 1 shall apply accordingly.
3. Participants shall either:
 - 1) ensure due protection of personal data used by authorised persons to login a KDPW application and provide such persons with conditions necessary to duly secure the devices used by such persons to login the application and to protect such devices from malware or unauthorised access; or
 - 2) check on an on-going basis whether the means and measures used by the authorised person to ensure protection of data used by such person to login a KDPW application and to protect the devices used by such person to login the application from malware or unauthorised access are adequate and ensure the necessary level of such protection.

4. The risk of the selection of protection measures or security means applied to protect data and devices referred to in subpara. 3 point 1 or 2 shall be solely with the participant. If the protection measures or security means applied to protect data and devices referred to in subpara. 3 point 1 or 2 provide insufficient or defective for any reason, the participant shall have sole liability for any consequences. Such liability shall arise irrespective of the participant's fault.
5. KDPW shall not be liable for the acts or omissions of persons authorised by a participant, in particular for the loss or sharing of login data by such persons with third parties.

§ 11

1. Access to a KDPW application may be revoked:
 - 1) by KDPW if the participant revokes the authorisation granted to a person referred to in § 7 subpara. 7 point 1 or 2;
 - 2) by KDPW if the participant reports:
 - a) suspicion of access to a KDPW application using the access account by an unauthorised person,
 - b) breach of data used to log in to a KDPW application,
 - 3) by a person authorised by a participant as administrator by withdrawing access to the KDPW application from the person referred to in § 7 subpara. 7 point 1.
2. Revocation of the authorisation referred to in subpara. 1 point 1 shall be effective for KDPW after the end of a period of two business days following the day when participant's statement to that effect is delivered to KDPW in writing or electronically (in the form of a document bearing a qualified electronic signature).

Section 4

Rights Administrator

§ 11a

1. The regulations of a particular service may indicate that a participant with a given participation type shall be obliged to appoint a rights administrator. In such instances, the participant shall be obliged to authorize at least one person to act on its behalf as the rights administrator.
2. The rights administrator shall be a person authorized by the participant to manage access to applications in which the participant uses or will be using in the future in its relations with KDPW, which on the date of the granting of the authorization to the participant shall be assigned by KDPW to a group of services appropriate for a given participation type, and access to other applications that will be assigned by KDPW to this group of services in the future.
3. Management of access rights to the application by the administrator shall be understood to mean the granting of rights to other persons authorized by the participant to communicate with KDPW, as a service administrator or user, as well as revoking such rights by, respectively, granting or revoking access to a specific application, and in instances where the participant acts within a given service on behalf of another entity or other entities - also to act in the abovementioned scope on behalf of these other entities.
4. Gaining access to the KDPW applications included in the service group by a person acting as a service administrator or user, or withdrawing access to the KDPW application from such a person, may only be performed by the rights administrator acting on behalf of this participant.

5. Obtaining access to access management by the rights administrator shall require the submission of personal data identifying the person authorized by the participant, these being: the PESEL number - in the case of persons with Polish citizenship, or date of birth - in the case of persons with non-Polish citizenship.

6. Obtaining access to access management by the rights administrator shall require an access account and submission of an application.

7. Submitting an application shall involve:

1) completion by a person authorized by the participant of a dedicated online form available on the Services Portal, and

2) providing KDPW with a declaration submitted by the participant on granting this person authorization to act on its behalf within the scope indicated in this declaration and confirming the personal data of this person indicated by them in the form, referred to in point 1.

8. The participant shall submit the declaration, referred to in subpara. 7 point 2, to KDPW in writing or in electronic form (in the form of a document with a qualified electronic signature).

9. KDPW shall accept or reject the application after its formal and substantive verification.

Chapter 3

Repealed

Chapter 4

Final provisions

§ 18

1. KDPW may amend these rules.
2. KDPW shall make any amendment to these rules available to participants on its website. Amendments shall come into effect within two weeks from the date on which they are made available, unless the resolution of the KDPW Management Board introducing the amendments indicates a later effective date.
3. Any amendment of these rules and its effective date shall be notified to participants within the time limit referred to in subpara. 2.
4. The transmission of information concerning amendments to the Rules via email sent to the email address of a person authorised by a participant to access a KDPW application shall be deemed to have been the legally effective delivery of the notification of the amendment to the participant, unless otherwise stated in the provisions of the rules of the service.
5. If a participant refuses to accept an amendment of the rules, the participant may terminate the service agreement with KDPW subject to the conditions of termination under the service rules.

6. Unless a participant terminates the participation agreement according to subpara. 5, the participant shall be deemed to accept the amendment of the rules if notified according to subpara. 3 and 4.