RULES OF ACCESS TO THE IT SYSTEMS OF KRAJOWY DEPOZYT PAPIERÓW WARTOŚCIOWYCH

Chapter 1

General

§ 1

1. These rules of access to the IT systems of Krajowy Depozyt Papierów Wartościowych, hereinafter the "rules", set out the rules of access to and authorisation in the KDPW applications dedicated to electronic communication with KDPW and the rules required to set up a system connection with the KDPW applications.
2. These rules apply in legal relations arising from agreements concluded by KDPW with participants or other entities which receive services provided by KDPW that are available via KDPW's IT systems.

§ 2

Whenever the following terms are used in these rules:

1) KDPW application – this shall be understood to mean the IT system used in a service provided by KDPW, enabling the exchange of information or messages between a participant and KDPW using data transmission;
2) access application – this shall be understood to mean an application enabling access to a KDPW Group application based on a single sign-on (SSO), available on the website of KDPW and of KDPW's subsidiary;
3) service – this shall be understood to mean a service provided by KDPW or functionalities available to participants via a KDPW application;
4) participant – this shall be understood to mean an entity which is a party to a participation agreement concluded under the KDPW 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 other than services;
5) 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;
6) message – this shall be understood to mean information which, under the service rules, in relations between a participant and KDPW, may or should be transmitted via means of electronic communication;
7) electronic communication – this shall be understood to mean the exchange of messages between a participant and KDPW or the participant's gaining access to information via a KDPW application;
8) KDPW – this shall be understood to mean the company Krajowy Depozyt Papierów Wartościowych S.A.;
9) KDPW Group – this shall be understood to mean KDPW and the subsidiaries of KDPW;
10) business day – this shall be understood to mean any day of the week which is not a statutory holiday or a Saturday.

§ 3

1. Electronic communication with the KDPW applications is available via the following

communication interfaces:

1) U2A, which is a graphical user interface supporting manual exchange of data with a KDPW application; or
2) A2A, which is an interface supporting automated exchange of data between a KDPW application and a participant's application.

2. The communication interfaces are defined independently for each service in accordance with the terms and conditions of communication defined for the service.

3. Data provided to KDPW via U2A shall be deemed delivered upon the confirmation of their effective logging by a KDPW application.

4. Data provided to KDPW via A2A shall be deemed delivered upon the participant's transmission of a message containing such data unless the message is rejected following checks. A message shall be deemed delivered upon its entry into the input message queue in the communication channel dedicated to the service.

5. The terms and conditions of communication defined for each service may impose additional obligations on participants in connection with the transmission of messages, in particular the obligation to sign messages with an electronic signature.

Chapter 2

Electronic communication via U2A

Section 1

Access account

§ 4

1. Electronic communication with KDPW via U2A requires an access account to be opened in the access application.

2. An access account in the access application is opened by a natural person acting on his or her own behalf by completing a dedicated access 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 submission of an application for access to the KDPW application; withdrawal of the consent shall result in the access account being closed. An access account may be opened following the verification of the email address provided in the form, which the person opening the account shall confirm with 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).

4. Details of how to open and use an access account are available in the account user manual published on the KDPW website.

5. In the case of an access account of a person who gains access to a KDPW application on behalf of a user, the participant shall immediately notify KDPW of any breach of personal data used by such person to login the KDPW application and, if necessary, request KDPW to block such person's

access account.

6. 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.

7. KDPW shall block an access account:
1) if a participant reports suspected unauthorised access to a KDPW application using the access account;
2) if a participant requests the account to be blocked according to subpara. 5;
3) if the maintenance of the account poses a threat to the security of KDPW's IT systems;
4) if required by law.

8. 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 from the access application and revoke access to the KDPW application.

9. KDPW shall immediately notify a participant that an access account has been blocked and explain the reasons.

Section 2

Authorisation in the KDPW application

§ 5

1. A person holding an access account gains access to the KDPW application based on a request.

2. A request is submitted as follows:
1) the person authorised by the participant completes a dedicated online form available in the access account opened by such person in the access application; and
2) the participant delivers 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.

3. The statement referred to in subpara. 2 point 2 shall be provided by the participant to KDPW in writing in the original counterpart or a scan, depending on the type of service. Details of how to deliver the statement shall be provided to the person authorised by the participant after completing the form referred to in subpara. 2 point 2 in an email message generated by the access application.

4. Access to a KDPW application may also be granted on the basis of existing access where:
1) a new KDPW application is developed, replacing an application previously used to support a service, by granting access to such application through a transfer (migration) of existing permissions of a person authorised by a participant to use the service;
2) KDPW opens a new service, by granting access to the new KDPW application automatically to a person authorised to use another service; in that case, the person requesting access to a KDPW application is notified of granted access automatically in an email message generated by the access application.

5. The request referred to in subpara. 2 shall be presented no later than 5 business days before the date when the person authorised by the participant wishes to send or receive a message via a

KDPW application.

6. A request may concern the permission for the person authorised by the participant to:
1) communicate directly with KDPW on behalf of the participant (user role); or
2) grant to other persons who complete the form referred to in subpara. 2 point 1 for access to the KDPW application, to the extent defined in point 1, the permission to communicate directly with KDPW on behalf of the participant and to revoke such permission by granting or revoking, respectively, their access to the KDPW application (administrator role).

7. Subject to § 6, KDPW shall accept or reject requests following formal and content checks of the statement referred to in subpara. 2 point 2.

8. Requests may be rejected after a time limit, which shall be no less than 30 days after the completion of the form referred to in subpara. 2 point 1, failing its approval by KDPW within such time limit.

9. If a request is rejected, a new request must be filed to gain access to the KDPW application.

§ 6

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 § 5 subpara. 6 point 2 (administrator role). In that case, participants shall authorise at least one person to act on their behalf as 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 administrator.

§ 7

1. When logging in the access application, access account holders shall be authenticated to use all KDPW Group applications to which they have access, available in the access application. Authentication shall be performed on the basis of the entered access account login and password.

2. The list of services available to access account holders shall be updated upon each application access login.

3. If access to a KDPW application is granted during the user's active session, the access account holder may use such access after closing the session and logging in once again.

4. A user's access to services shall be verified during an access session. Failure to confirm access shall result in revocation of access to the service.

§ 8

1. Persons granted access to a KDPW application as users in connection with the participant's presentation of the statement referred to in § 5 subpara. 2 point 2 or a permission granted to them under § 5 subpara. 6 point 2 shall be deemed authorised to communicate directly with KDPW and actions of such persons shall be deemed actions of the participant. The preceding sentence shall apply also where the form or certificate referred to in § 5 subpara. 2 contains incorrect personal data of the person concerned.

2. Persons granted access to a KDPW application as administrator in connection with the participant's

presentation of the statement referred to in § 5 subpara. 2 point 2 shall be deemed authorised to grant permissions to communicate directly with KDPW. 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. Participants shall regularly review the permissions of persons authorised to access a KDPW application on their behalf.

§ 9

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 § 5 subpara. 6 point 1 or 2;
2) by KDPW if an access account is blocked according to § 4 subpara. 5, 7 or 8;
3) by a person authorised by a participant as administrator if the participant revokes the authorisation granted to a person referred to in § 5 subpara. 6 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 written statement to that effect is delivered to KDPW.

Chapter 3

Electronic communication via A2A

§ 10

1. A2A is an electronic communication system dedicated to supporting automated communication, used to exchange messages in real time with technical means ensuring protection of confidentiality and integrity of transferred information and sender non-repudiation.

2. Communication via A2A relies on message queues set up in each communication channel.

3. Message queues may be established independently for each KDPW application. A communication channel may be used to access more than one KDPW application by means of dedicated queues.

4. All queues available in A2A are set up in accordance with the service rules and the terms and conditions of communication defined for each service. Communication is established by setting up pairs of queues separately for each direction of communication.

5. Message queues can be accessed after access to the communication channel for such queues is authenticated with an electronic certificate downloaded by the user. Communication in a communication channel is secured with TLS encryption.

6. Connectivity with the KDPW infrastructure is available in the client-to-server and the server-to-server model. VPN connections are required with pre-shared key authentication.

§ 11

1. Subject to subpara. 2, communication via A2A is available to participants 24/7.
2. Interruptions in the availability of message queues may result from:
1) scheduled interruptions in the operation of a service announced in accordance with the service rules or the terms and conditions of communication defined for a service;
2) technical breaks of several minutes each necessary to reconfigure message queue parameters.
3. Participants shall configure automatic reconnection to message queues in their systems.
4. KDPW reserves the right to delete unreceived messages from message queues 30 days after the message is sent or within a shorter time limit if so agreed with the participant.

§ 12

1. Electronic communication via A2A requires the user to download an electronic certificate.

2. To download an electronic certificate, the person authorised by the participant shall complete a dedicated form published on the KDPW website with the data required in the form and the participant shall deliver to KDPW a written statement accepting the finality of delivery of messages using such certificate. KDPW shall deliver the certificate to the participant at the email address provided in the form and confirmed by the participant in the delivered statement.

3. Electronic certificates are used to authenticate participants submitting messages using such certificate to a dedicated communication channel.

4. KDPW and participants shall accept the finality of delivery of messages authenticated with electronic certificates referred to in subpara. 1 and they shall consent to the gathering of all potential evidence that this action has been performed.

5. Participants shall save downloaded electronic certificates in a manner allowing only authorised access to such certificates. From the time of downloading a certificate until the certificate is revoked, the risk of loss or disclosure of the certificate is solely with the participant.

§ 13

1. Subject to subpara. 4, electronic certificates shall be valid within the term defined in the certificates.

2. Participants shall regularly monitor the validity of downloaded electronic certificates. Participants

shall request KDPW to issue a new electronic certificate no later than 10 business days before the expiry date of the certificate.

3. KDPW may, before the expiry of the term referred to in subpara. 1, revoke an electronic certificate by its own initiative for technical reasons, at the request of the participant or due to suspected unauthorised use of the electronic certificate.

4. KDPW shall make available to participants, on its website, the certificate revocation list (CRL) necessary to check the validity of certificates. Revocation of a certificate shall be added to the list immediately after the electronic certificate is revoked.

5. If an electronic certificate is revoked, KDPW shall immediately notify the participant thereof at the email address provided in the form referred to in § 12 subpara. 2.

§ 14

1. If an electronic certificate is lost or there is reasonable suspicion of unauthorised access to the electronic certificate, the participant who downloaded the electronic certificate shall immediately request KDPW to revoke the electronic certificate and explain the reasons for such revocation.

2. An electronic certificate shall be revoked for the reasons referred to in subpara. 1 immediately upon receipt of a revocation request concerning such certificate.

3. KDPW shall not be liable for any damage caused to participants in connection with the loss of an electronic certificate during its validity.

§ 15

KDPW is not a qualified trust service provider within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (EU Legal Journal L 257, p. 73). In connection with the foregoing, certificates referred to in § 12 are not qualified certificates for electronic signatures within the meaning of this Regulation. This shall mean in particular that authentication of messages with these certificates does not have the legal effect of a hand-written signature within the meaning of the aforementioned Regulation and within the meaning of Article 78^1 sub-paragraph 2 of the Civil Code.

Chapter 4

Final provisions

§ 16

1. KDPW may amend these rules.

2. KDPW shall make any amendment to these rules available to participants by publishing it on its website no later than 14 days before the effective date.

3. Any amendment of these rules and its effective date shall be notified to participants.

4. Transmission of information concerning an amendment of the rules by email at the email address of a person authorised by a participant to access a KDPW application shall be deemed effective

delivery to the participant.

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.