KDPW

consolidated text as at 1 November 2022 as approved
in Resolution No. 166/16 of the KDPW Management Board
dated 11 March 2016, effective as of 11 March 2016,
incorporating amendments approved in the following Resolutions:
No. 699/16 dated 25 October 2016 effective as of 14 November 2016,
No. 861/17 dated 18 December 2017 effective as of 3 January 2018,
No. 316/2018 dated 23 May 2018 effective as of 6 June 2018,
No. 383/2018 dated 18 June 2018 effective as of 2 July 2018,
No. 321/2019 dated 18 June 2019 effective as of 1 July 2019,
No. 22/2020 dated 14 January 2020 effective as of 3 February 2020,
No. 750/2020 dated 14 August 2020 effective as of 28 August 2020
No. 512/2022 dated 8 June 2022 effective as of 1 July 2022,
with the exception of the provisions of § 1 point 4, 5 and 7,
which are valid from 1 November 2022

INFORMATION EXCHANGE SYSTEM RULES

§ 1.

1. The Information Exchange System Rules, hereinafter the "SWI Rules", shall apply with respect to legal relations deriving from SWI Agreements concluded between KDPW and SWI participants, as well as to legal relations between an SWI participant and KDPW deriving from the agreement on participation in the investor compensation scheme or ARM system participation agreement.

2. The SWI Rules shall define, in particular, the electronic communication systems which may be used to exchange documents in electronic form between a SWI participant and KDPW, the terms and conditions of use of such systems as part of the SWI, the principles for the identification of the users of these systems, accepted in the SWI, as well as the measures used in the SWI to ensure the security of the exchange of documents via such systems, including the rules of submission of declarations and transmission of documents in electronic form.

I. Definitions and abbreviations

§ 2.

The definitions and abbreviations used in the SWI Rules shall be construed as follows:

1) **Information Exchange System (SWI)** – means a set of technical and IT tools, which enable the submission of declarations of intent and sending of other information by means of electronic data transmission between KDPW and SWI Participants, using the electronic communication systems referred to in points 3-5 and – with respect to the systems described in points 3 and 4 – security measures generated and issued in accordance with the provisions of the SWI Rules;

2) **KDPW** – means the company Krajowy Depozyt Papierów Wartościowych S.A.;

3) **ESDI/WEB** – means the electronic communication system referred to in § 3, administered by KDPW;

4) **ESDK** – means the electronic communication system referred to in § 4, administered by KDPW;

5) **SWIFT Message Processing System** – means the electronic communication system organised on the basis of the SWIFT telecommunication network administered by the Society for Worldwide Interbank Financial Telecommunication with its head office in Belgium, referred to in § 5;

6) **Party's electronic signature** – means data in electronic format attached to a document as the signature of the person being the sender of the document and subject to cryptographic transformation which allow for the person submitting the signature to be identified, as well as the verification of the authenticity of the message. Electronic signatures are generated by means of algorithms referred to in Appendix 1;

7) **verification of message authenticity** – means the process of verifying the integrity of a document by means of authentication whether the message has not been subject to unauthorised modification, i.e., whether the content of the received message is the same as the content of the sent message, performed by comparing the hash function value of the document with the value calculated and indicated by KDPW (in the case of ESDI/WEB) or by verifying the authenticity of the electronic signature (in the case of ESDK). As a result of the verification of the authenticity of the message, information is also obtained on the basis of data from the authentication process with a certificate (in the case of ESDI/WEB) or on the basis of an electronic signature (in the case of ESDK), on whether the sender of the message is who they claim to be. Verification of message authenticity is deemed negative if the message content has been distorted (message integrity has been breached), or if the sender of the message is not who the sender claims to be, while for messages with an electronic signature attached, also when the sender's electronic signature was not valid at the time of the delivery of the message to the recipient;

8) **documents** – means documents within the meaning of the SWI Agreement;

9) **system documents** - means documents that are generated directly from the IT system used, respectively, by KDPW to operate the depository system, the investor compensation scheme, the ARM, or that are generated directly from the IT system used by KDPW_CCP to operate the transaction clearing system, or documents which are registered directly in any of these IT systems, in particular, in relations between KDPW and SWI participants that are direct participants of the depository system operated by KDPW, settlement instructions and other registration instructions described in the KDPW Detailed Rules of Operation;

10) **Chief Guarantor** – means the person being an employee of KDPW appointed by the Management Board of KDPW who has the function of trusted third party in the ESDI/WEB and ESDK systems, generates security measures, and guarantees that the document sender and recipient in the systems are who they claim to be. The Chief Guarantor performs the Certification Authority function in the systems by means of cryptographic hardware modules used to generate private cryptographic keys and public cryptographic keys;

11) **SWI Agreement** – means the Agreement concerning presentation of declarations and transmission of documents in electronic form, concluded between an SWI Participant and KDPW, of which the SWI Rules are an integral part;

12) **SWI Participant** – means a participant of the depository system operated by KDPW, a participant of the transaction clearing system operated by KDPW_CCP S.A., a Pension Fund Company, an Open Pension Fund or any other entity which is a party to an SWI Agreement concluded with KDPW.

II. Electronic communication systems in SWI

§ 3.

ESDI/WEB

1. The scope of application of ESDI/WEB:

   1) the system is dedicated to data exchange using online application mechanisms via internet communication channels. Data exchange is manual (user-to-system) in the web browser or automated (system-to-system) via the SWI Participant's IT system.

   2) ESDI/WEB allows SWI Participants to send the following to KDPW:

      a) system documents in KDPW XML and fixed-field format, transmitted manually by the SWI Participant in the web browser to KDPW's IT system;

      b) system documents in KDPW XML and fixed-field format, transmitted automatically from the SWI Participant's IT system to KDPW's IT system;

      c) communication documents (in any format), transmitted by the SWI Participant to KDPW's organisational units;

   3) ESDI/WEB allows KDPW to send the following to SWI Participants:

      a) system documents in KDPW XML and fixed-field format, transmitted from KDPW to SWI Participants. Access to documents is available in the web browser or the SWI Participant's IT system;

      b) communication documents (in any format), transmitted by KDPW's organisational units to SWI Participants. Access to documents is available in the web browser or the SWI Participant's IT system;

   4) KDPW publishes on its website the scope and structure of KDPW proprietary XML and fixed-field messages, which may be transmitted as part of the SWI using the ESDI/WEB system.

2. ESDI/WEB supports the exchange of messages in electronic form via a dedicated website available at www.kdpw.pl using technical means ensuring the confidentiality and integrity of data transmission and non-repudiation of the sender. Security mechanisms used in ESDI/WEB are based on recognised standards of cryptographic security of data transmission and use of tools to verify the authenticity of messages. The ESDI/WEB system is comprised of the following components:

1) central system (website server) which supports the transmission and receipt of electronic documents between KDPW and SWI Participants;

2) SWI Participants' client stations equipped with a web browser or other client software necessary for communication of users with the central system.

3. Rules of operation

1) documents sent to KDPW via ESDI/WEB are considered recorded in the system at the time of the sender's receipt of confirmation of delivery of the document to the recipient. Confirmation of document delivery is a special message esdk.acc.001.01 sent by the ESDI/WEB system to the sender;

2) documents sent from KDPW via ESDI/WEB are considered recorded in ESDI/WEB at the time of receipt in the central system.

§ 4.

ESDK

1. The scope of application of ESDK:

1) the system is used for high traffic data exchange, automated (system-to-system), using MQ queuing mechanisms via dedicated digital communication channels;

2) ESDK allows SWI Participants to send to KDPW system documents in KDPW XML format, transmitted on-line from the SWI Participant's IT system to KDPW's IT system;

3) ESDK allows KDPW to send to SWI Participants system documents in KDPW XML format, transmitted on-line from KDPW's IT system to the SWI Participant's IT system;

4) KDPW publishes on its website the scope and structure of KDPW proprietary XML messages, which may be transmitted as part of the SWI using the ESDK system.

2. ESDK is a system of electronic communication between KDPW and SWI Participants dedicated to support automated (system-to-system) communication. It is designed to support exchange of messages in real time using technical means ensuring the confidentiality and integrity of data transmission and non-repudiation of the sender. Security mechanisms used in ESDK are based on recognised standards of cryptographic security of data transmission and use of electronic signatures. ESDK supports the exchange of standard messages in real time using WebSphere MQ Server queuing mechanisms. The ESDK system is comprised of the following components:

1) ESDK server – the interface between KDPW's IT system and SWI Participants' IT systems; the ESDK server was developed on the WebSphere MQ Server platform; its function is to sign and send messages generated by KDPW's IT system to SWI Participant input queues and to receive and verify messages from SWI Participant output queues and transmit them to KDPW's IT system;

2) ESDK Client – software used in the SWI Participant's IT system to exchange messages with the ESDK Server via input and output queues. Client application access to message queues is provided by a Websphere MQ program interface.

3. Rules of operation:

1) (*Repealed)*

2) (*Repealed)*

3) documents sent to KDPW via ESDK are considered recorded in the system at the time of the sender's receipt of confirmation of delivery of the document to the recipient. Confirmation of document delivery is a special message esdk.acc.001.01 sent by the ESDK system to the sender. Confirmation of document rejection is a message esdk.rjc.001.01 sent by the ESDK system to the sender;

4) documents sent from KDPW via ESDK are considered recorded at the time of receipt in the SWI Participant output queue on the ESDK server;

5) at the request of SWI Participants, copies of system documents transmitted by KDPW to the SWI Participant may at the same time be transmitted to another ESDK user named by the SWI Participant.

§ 5.

SWIFT Message Processing System

1. Scope of application:

1) the system is used for automated (system-to-system) or manual (user-to-system) data exchange using advanced services of the SWIFT network operator;

2) the SWIFT Message Processing System allows SWI Participants and KDPW to exchange system documents in SWIFT messages, transmitted between the SWI Participant's IT system and KDPW's IT system;

3) KDPW publishes on its website the list of SWIFT services used and the scope of SWIFT messages which may be transmitted between SWI Participants and KDPW in the SWIFT Message Processing System. The structure of SWIFT messages must conform to the SWIFT network standard but KDPW may define specific rules of completing messages.

2. Technical description:

1) the solution is dedicated to automated (system-to-system) or manual (user-to-system) data exchange;

2) the communication layer of the solution is based on interactive SWIFT messaging services;

3) the confidentiality, integrity and non-repudiation of data transmission in the communication channel is ensured by mechanisms used by SWIFT which are based on recognised standards of cryptographic security of data transmission;

4) the solution is consistent with the recommendations of the Giovannini Group responsible for standardising data exchange on the international capital market.

3. (*Repealed)*

III. Transmission of documents as part of the SWI using the ESDI/WEB and ESDK system

§ 6.

1. The activation of document exchange via ESDI/WEB or ESDK requires the SWI Participant to submit to KDPW the following documents:

   1) written powers of attorney granted according to the template presented in Appendix 2 to the SWI Rules, indicating the person authorised to submit declarations of intent on its behalf and to transmit documents via ESDI/WEB or ESDK, respectively; instead of a power of attorney, the SWI Participant may provide KDPW with a valid copy of an entry from the relevant company register if the person referred to in the preceding sentence, is a person authorised to represent it under single-representation rules and is entered in the register;

   2) certification form according to the template presented in Appendix 3 to the SWI Rules, completed by the person referred to in point 1 above; furthermore, such person shall provide a written declaration of authorisation of the private cryptographic key given to that person in the wording presented in Appendix 4 to the SWI Rules, where this declaration should be signed in the presence of the Chief Guarantor

2. SWI Participants shall monitor on an on-going basis the validity of the data provided in certification forms presented to KDPW for persons acting on their behalf under powers of attorney referred to in sub-paragraph 1 point 1, and immediately provide such persons with the contents of the SWI Agreement and the SWI Rules as well as any amendments thereof.

3. SWI Participants shall not change the scope of authorisation arising from powers of attorney granted by it, referred to in sub-paragraph 1 point 1.

4. SWI Participants shall give the Chief Guarantor at least a one-day written notice of the date of expiration or revocation of the power of attorney referred to in sub-paragraph 1 point 1. If this deadline cannot be respected, the notice shall be given immediately after the expiration or revocation of the power of attorney.

5. SWI Participants shall have exclusive liability for the legal consequences of failure to perform or undue performance of the obligation referred to in sub-paragraph 4.

§ 6a.

(Repealed)

§ 7.

1. Documents prepared in the form of computer files, including system documents prepared in XML format, may be transmitted between the parties to the SWI Agreement via ESDI/WEB.

2. Only system documents may be transmitted between the parties to the SWI Agreement via ESDK. Transmission of documents other than system documents via ESDK shall have no legal effect.

§ 8.

1. Documents transmitted via ESDK shall be signed with the party's electronic signature which identifies the person presenting the declaration on behalf of the party the SWI Agreement.

2. Documents transmitted via ESDI/WEB shall be sent by an authenticated person using a certificate.

3. Failure to comply with the obligation referred to in sub-paragraph 1 or 2 shall be tantamount to failure to comply with the form reserved in the SWI Rules for presentation of declarations of intent and transmission of other declarations or information via ESDI/WEB or ESDK and shall result in ineffective delivery of the declaration or information contained in the document to the other party to the SWI Agreement.

4. Verification of the authenticity of a message sent by ESDK shall be performed by the document recipient party with the public cryptographic key of the sender party, which is public information generated according to the algorithm described in Appendix 1 to the SWI Rules, which enables identification of the sender party by the person presenting a declaration on behalf of that party. Negative verification of message authenticity shall cause its rejection by the Information Exchange System. In case of negative verification of message authenticity, the declaration of the sender shall be considered not presented and the document shall be considered not delivered to the other party to the SWI Agreement. The document recipient party shall immediately notify the sender party of each such case.

5. Verification of the authenticity of the message sent by ESDI/WEB is performed using the hash specified in the ESDI/WEB and comparing it with the value generated by the party being the sender, based on the appropriate algorithms and own or independent vendor tools. Each party should notify the other about any instances of identified irregularities.

§ 9.

1. In case of detection of any distortions, errors or other irregularities in the content of a delivered document originating during its transmission, the recipient party shall immediately notify the sender party thereof.

2. Neither party to the SWI Agreement shall be liable for losses incurred by the other party to the SWI Agreement as a result of any failure of ESDI/WEB or ESDK or in connection with the operation of the systems or as a result of any failure of means of communication between the parties; however, liability for losses shall not be excluded if a party:

   1) fails to notify the other party immediately of negative verification of message authenticity or a detected error, distortion or other irregularity in the content of a document according to the obligations referred to in sub-paragraph 1 or § 8 sub-paragraph 3; or

   2) through its failure to exercise due diligence, fails to detect an error, distortion or other irregularity in the content of an electronic document referred to in sub-paragraph 1.

§ 10.

If the transmission of documents via ESDK is not possible, the parties to the SWI Agreement shall use another electronic communication system activated by the SWI Participant.

IV. Security measures applied in ESDI/WEB and ESDK as part of the SWI

§ 11.

1. Neither KDPW nor the Chief Guarantor are qualified trust service providers 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. In connection with the foregoing, certificates issued by the Chief Guarantor are not qualified certificates for electronic signatures within the meaning of this Regulation. This shall mean in particular that an electronic signature verified 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.

2. The Management Board of KDPW shall appoint Deputy Chief Guarantors from among employees of KDPW to perform Chief Guarantor functions in the absence of the Chief Guarantor. The provisions of the SWI Rules concerning the Chief Guarantor shall apply accordingly to Deputy Chief Guarantors.

§ 12.

1. The security measures designated for the parties to the SWI Agreement, referred to in Appendix 1 to the SWI Rules, i.e.:

   1) certificates containing private cryptographic keys together with the public cryptographic keys of the party (ESDI/WEB certificates, ESDK certificates and a TLS connection as part of the MQ software architecture between KDPW and the SWI Participant);

   2) certificates of the Certification Authority containing the public keys of the Certification Authority;

3) security passwords;

shall be generated by the Chief Guarantor.

2. The security measures referred to in sub-paragraph 1 points 1-3 shall be generated separately for the purpose of transmission of documents via ESDI/WEB and ESDK.

3. Certificates available to the Parties to the SWI Agreement from the Chief Guarantor shall contain, in addition to the relevant public key, also additional information necessary to identify the certificate owner, identify the issuer, identify the certificate validity and identifier, and information about the algorithm, authenticated by the Certification Authority in the form of an electronic signature generated using the private cryptographic key of the Certification Authority.

§ 13.

1. "The security measures, designated to a party to the SWI Agreement, generated by the Chief Guarantor and recorded on relevant media shall be given out by the Chief Guarantor at the head office of KDPW to a person authorised by the party in writing to collect them. As of the moment of collection, the risk of their accidental loss or disclosure rests exclusively with the party to the SWI Agreement which has received them.

2. A private cryptographic key may only be given to a person which is to be identified in the Information Exchange (SWI) System by means of this key, and which has been indicated in the power of attorney granted by the party to the SWI Agreement in accordance with § 6 sub-paragraph 1 point 1, or – in instances where the SWI Participant has obtained internet security measures – to a person authorised by name by the SWI Participant indicated in the certification form.

3. SWI Participants shall keep secret all received private cryptographic keys, security passwords and create conditions which enable persons to whom they have granted powers of attorney referred to in § 6 sub-paragraph 1 point 1 to ensure their secure storage including without limitation protection against loss, destruction and unauthorised access.

§ 14.

1. KDPW shall create conditions which enable the Chief Guarantor to keep strictly confidential all private cryptographic keys and security passwords generated by the Chief Guarantor.

2. The Chief Guarantor shall not keep copies of private cryptographic keys and security passwords given to SWI Participants.

§ 15.

1. Cryptographic keys and certificates shall expire on the expiration date of the certificate, subject to § 16 sub-paragraph 2 first sentence.

2. The transmission of a document after the expiration date of the private cryptographic key contained in the certificate shall have no legal effect and in particular it shall not result in effective presentation of the declaration or delivery of information contained in the document.

3. The Chief Guarantor shall give new cryptographic keys, certificates and security passwords at the head office of KDPW to a person authorised by the party to the SWI Agreement in a power of attorney referred to in § 6 sub-paragraph 1 point 1 at a date agreed by such person with the Chief Guarantor.

4. New cryptographic keys and certificate replacing those previously used by SWI Participants may also be given upon the registration of a request generated using valid existing cryptographic keys and certificate. In that case, new cryptographic keys and certificate shall be given upon their download from the website https://cert.kdpw.pl. Requests shall be filed and new cryptographic keys and certificate shall be downloaded according to the procedure defined on that website.

5. The provisions of sub-paragraph 4 shall not apply if the certification form presented to KDPW for a person who is a proxy of the SWI Participant contains invalid data of such person. In that case, the SWI Participant shall take measures preventing such person from registering a request referred to in sub-paragraph 4 and – if the power of attorney granted to such person is to remain effective – ensuring that new cryptographic keys and certificate shall be given to such person according to sub-paragraph 3.

6. The provisions of § 6 sub-paragraph 1 and § 12—14 shall apply accordingly to giving new cryptographic keys and certificates.

7. The provisions of sub-paragraphs 3-5 shall not apply to issuing new internet security measures. The issue of new internet security measures shall require the submission by the SWI Participant of an application in the form of a certification form, completed and sent using the www.kdpw.pl web portal and the delivery to KDPW of a written declaration submitted on behalf of the SWI Participant by persons authorised to represent that SWI Participant, confirming the validity of the data contained in the form.

§ 16.

1. In case of reasonable suspicion of disclosure or breaking of a private cryptographic key, the party to the SWI Agreement for which the key has been generated and to which it has been given should request the Chief Guarantor in writing to replace its existing keys, certificate and security passwords used by it together with a justification.

2. Immediately on the receipt of a request referred to in sub-paragraph 1, the Chief Guarantor shall revoke the existing certificate used by the requesting party and the related keys and security passwords. The provisions of § 15 sub-paragraph 2 shall apply accordingly.

3. Information about the revocation of a certificate shall immediately be published by the Chief Guarantor on the website www.kdpw.pl.

4. Until the party making a request referred to in sub-paragraph 1 is given new keys, certificate and security passwords, all documents addressed to that party and originating from that party shall be delivered only using security measures which are not to be replaced, and where all keys, certificates and security passwords used by that Party are to be replaced, then via the SWIFT Message Processing System if it has been activated between the Parties pursuant to § 19 sub- paragraph 1 and the delivered document is a system document which may be transmitted between the Parties via such system.

5. The provisions of sub-paragraphs 1-4 shall apply accordingly in the event of any circumstances which require any change of data contained in the certificate given to a party to the SWI Agreement.

V. Transmitting and receiving documents through the mediation of another legal person

§ 17.

1. SWI Participants may perform all actions related to the transmission and receipt of documents via ESDI/WEB or ESDK through the mediation of another legal person. In that case, the SWI Participant shall grant to such legal person a power of attorney according to the template presented in Appendix 2a to the SWI Rules.

2. In the event referred to in sub-paragraph 1, the exchange of documents via ESDI/WEB or ESDK shall require actions referred to in § 6 sub-paragraph 1 to be performed, respectively, by the legal person authorised by the SWI Participant in a power of attorney referred to in sub-paragraph 1 and by a natural person who is the SWI Participant's further proxy. The template of the power of attorney for the SWI Participant's further proxy is presented in Appendix 2b to the SWI Rules.

3. In the event referred to in sub-paragraph 1, the Chief Guarantor shall generate the security measures referred to in § 12 sub-paragraph 1 for the legal person authorised as a proxy of the SWI Participant. Such measures shall be given to the persons authorised as the SWI Participant's further proxies in compliance with § 13 sub-paragraphs 1-2, accordingly, and modified on the general terms, whereas in the event referred to in § 16 sub-paragraph 1, a request for modification of security measures may be made either by the SWI Participant or by a proxy authorised by the SWI Participant. Only the proxy authorised by the SWI Participant shall be notified by KDPW as referred to in § 8 sub-paragraph 3.

4. In the event referred to in sub-paragraph 1, documents sent by the SWI Participant via ESDI/WEB shall be authenticated on the basis of a certificate, while for ESDK, they shall be signed with the Party's electronic signature identifying the SWI Participant by its further proxy.

§ 17a.

1. Where the SWI Participant has been appointed as the account operator within the meaning of the KDPW Rules (hereinafter "Account Operator"):

   1) all documents transmitted by it on behalf of the participant of the depository system who has appointed it as the Account Operator should be in the case of ESDI/WEB sent using authentication on the basis of a certificate, while in the case of ESDK, signed with the electronic

signature of the Party generated with the certificate which identifies the represented participant of the depository system in ESDI/WEB or ESDK, respectively;

2) it should verify the authenticity of messages contained in documents transmitted via ESDI/WEB or ESDK and addressed to the participant of the depository system who has appointed it as the Account Operator with the certificate which identifies the represented participant of the depository system in ESDI/WEB or ESDK, respectively.

2. Certificates which identify the participant of the depository system represented by the Account Operator in ESDI/WEB or ESDK and other security measures referred to in § 12 sub-paragraph 1 which are linked to such certificates shall be generated by the Chief Guarantor under the SWI Agreement between the Account Operator and KDPW concerning its activity to that extent and on the basis of a power of attorney to request that they are handed over, to collect them and to use them in the electronic communication systems administered by KDPW, granted to the Account Operator by the participant of the depository system represented by the Account Operator.

3. The generation of the security measures referred to in sub-paragraph 2 shall require the submission of the following to KDPW:

1) a further power of attorney granted by the Account Operator according to the template in Appendix 2c to the SWI Rules, which names the natural person authorised to make declarations of intent and other declarations on behalf of the represented participant of the depository system via ESDI/WEB or ESDK, respectively;

2) the certification form completed by the natural person referred to in point 1 according to the template in Appendix 3 to the SWI Rules and the submission by the natural person of a written declaration of authorisation of the cryptographic key handed to him or her according to the template in Appendix 4a to the SWI Rules, which should be signed in the presence of the Chief Guarantor.

4. The security measures referred to in sub-paragraph 2 shall be generated for the natural person who is a further proxy of the represented participant of the depository system and handed to such natural person according to § 13 sub-paragraph 1 and 2, which apply accordingly.

5. The certificate of the Party referred to in subpara. 1 point 1 shall identify the participant of the depository system represented by the Account Operator via the further proxy.

6. The other provisions of the SWI Rules shall apply, as required, accordingly to the relations between KDPW and the Account Operator to the extent of such activity of the Account Operator, excluding however § 17, § 19 and § 20, which shall not apply.

VI. Software, terms of licence

§ 18.

(Repealed)

VII. SWIFT Message Processing System

§ 19.

1. The exchange of documents via the SWIFT Message Processing System requires communication connectivity to be set up between the SWI Participant and KDPW on the terms applicable to the relevant SWIFT service. Prior to setting up the connectivity, the SWI Participant shall present to KDPW a written declaration prepared according to the template presented in Appendix 5 to the SWI Rules.

2. Only system documents referred to in § 5 sub-paragraph 1 point 2 may be transmitted between the parties to the SWI Agreement via the SWIFT Message Processing System. Transmission of documents other than system documents via the SWIFT Message Processing System shall have no legal effect, subject to § 20.

3. Mutual identification of the parties to the SWI Agreement as senders and recipients of documents transmitted via the SWIFT Message Processing System shall be made by means of Bank Identifier Codes (BIC) identifying the Parties in the SWIFT network. The standard rules of transmission, encryption, signing with the Party's electronic signature and verification of message authenticity used in the SWIFT network shall apply to documents transmitted via this system.

4. Presentation of a declaration referred to in sub-paragraph 1 by the SWI Participant shall be tantamount to the SWI Participant granting KDPW irrevocable powers of attorney to act in full confidence as to the content of declarations contained in documents transmitted via the SWIFT Message Processing System and marked with the BIC identifying the SWI Participant, including without limitation:

   1) to consider such declarations to be declarations presented to KDPW by the SWI Participant, fully binding on the SWI Participant without the need for KDPW to make any examination of the identity or the scope of authority of the persons sending documents marked with the BIC identifying the SWI Participant;

   2) to take, on the basis of documents marked with the BIC identifying the SWI Participant, any actions which KDPW is authorised or required to take on the basis of such documents in accordance with the legislation or under separate agreements concluded with the SWI Participant.

5. KDPW shall have no liability for any losses incurred by the SWI Participant as a result of any actions taken by KDPW according to the authorisation given in sub-paragraph 4. In addition, KDPW shall have no liability to make any payments to third parties in respect of actions taken by KDPW on the basis of and in accordance with the authorisation given in sub-paragraph 4.

6. In the transmission of documents to KDPW via the SWIFT Message Processing System, the SWI Participant shall act only through the person identified by the SWI Participant in the declaration referred to in sub-paragraph 1 as the person authorised to present declarations of intent to such extent on behalf of the SWI Participant. The provisions of § 6 sub-paragraphs 4 and 5 shall apply

accordingly in case of revocation or expiration of such authorisation, and the SWI Participant shall immediately present to KDPW a new declaration referred to in sub-paragraph 1.

7. KDPW may make the acceptance of documents transmitted by the SWI Participant via the SWIFT Message Processing System and the execution of orders contained in such documents conditional on the provision of additional information by the SWI Participant or submission of relevant documentation as determined by KDPW, and may use other means of due diligence as required by or contributing to the attainment of objectives of relevant legal regulations concerning prevention of money laundering and financing of terrorism. Furthermore, KDPW may suspend the acceptance of such documents from the SWI Participant and suspend the execution of orders contained in such documents in cases defined in those legal regulations. KDPW shall have no liability for any losses incurred by the SWI Participant as a result of the use of any means referred to in the first sentence or in the second sentence.

8. Each of the parties to the SWI Agreement may, by presenting a unilateral written declaration to the other party with an advance notice of at least seven days, terminate the application of the provisions of sub-paragraphs 1-7. In that case, the other provisions of the SWI Agreement shall remain in force.

VIIa. Selecting an electronic communication system

§ 19a.

1. Documents are exchanged in the Information Exchange System via ESDI/WEB. At the request of a Participant, documents may also be exchanged via ESDK or the SWIFT Message Processing System. In that case, the Participant shall notify KDPW of the electronic communication system to be used by KDPW in order to transmit system messages to the Participant (default channel), subject to sub-paragraph 2.

2. If KDPW decides to set up a separate functional area within SWI, covering a specific group of system documents, the default channel for such functional area shall be selected by KDPW unless the Participant selects another default channel for such area.

3. KDPW shall publish on its website the functional areas, the default channels assigned to such areas, and the system documents assigned to the functional areas.

VIII. Communication between SWI Participants and KDPW_CCP S.A.

§ 20.

On the terms set out in Appendix 6 to the SWI Rules, for the duration of the SWI Participant's participation in the transaction clearing system operated by KDPW_CCP S.A., the Information Exchange System may be used by the SWI Participant to communicate with KDPW_CCP S.A.

IX. Final provisions

§ 21.

1. All appendices to the SWI Rules shall be an integral part of the SWI Rules.

2. KDPW may amend the SWI Rules.

3. The SWI Rules may be amended provided that the SWI Participant is notified in writing of the content and effective date of such amendment. The notification shall be given by sending the amendments in writing to the SWI Participant at the last address provided by the SWI Participant or electronically via ESDI/WEB.

4. If the SWI Participant does not accept an amendment of the SWI Rules, of which it is notified according to sub-paragraph 3, it may terminate the SWI Agreement with a one-month termination notice. The notice of termination shall be delivered to the head office of KDPW in writing within two weeks of the receipt of the notice referred to in sub-paragraph 3 by the SWI Participant.

5. Unless the SWI Participant delivers a notice of termination of the SWI Agreement to KDPW according to sub-paragraph 4, the SWI Participant shall be deemed to accept the amendment of the SWI Rules of which is notified according to sub-paragraph 3.

Appendix 1 to the SWI Rules

Security measures

The electronic communication systems are based on asymmetric cryptography services (public key cryptography). Depending on the electronic communication system activated by the SWI Participant, the SWI Participant has a unique set of security measures including:

1) certificates containing private cryptographic keys together with the public cryptographic keys of the party (ESDI/WEB certificates, ESDK certificates and TLS connectivity set up in MQ software between KDPW and the SWI Participant);

2) certificates of the Certification Authority containing the public keys of the Certification Authority;

3) security passwords;

KDPW also makes available repositories of certificate revocation lists (CRL) necessary to verify the validity of certificates. Certification Authority certificates are available in CER binary file format.

ESDI/WEB System

For the purposes of the ESDI/WEB system, KDPW issues certificates necessary to authenticate parties to the SWI Agreement. Certificates and private cryptographic keys issued for the ESDI/WEB system are provided to SWI Participants as PKCS12 files on external drives.

Security of messages transmitted via the ESDI/WEB system is ensured by account authentication based on electronic certificates. Certificates are issued and managed using KDPW's existing PKI (Certification Authority). Certificates are issued by the Certification Authority under X.509 v.3 and electronic signatures are generated under PKCS7 with the RSA asymmetric algorithm using at least 1,024 bit keys. ESDI/WEB system users are authenticated and authorised under TLS and certificates identifying the user in the system. TLS protocol guarantees data confidentiality and integrity in the transport layer. User authentication and authorisation in the system are based on security measures issued by KDPW.

In addition, the ESDI/WEB system will calculate from the document transferred to the system and show the participant the hash function value, which, based on the formerly adopted algorithm, the participant will be able to use to compare with the value that they will calculate themselves; if this value is the same as the value calculated by KDPW, it will be confirmation that the message has not been modified in an unauthorised manner.

ESDK System

For the ESDK system, KDPW issues certificates to set up TLS connectivity in MQ software, to authenticate SWI Participants in the ESDK system and to sign messages.

Certificates together with private cryptographic keys issued for the ESDK system are given to SWI Participants in PKCS12 files on portable carriers. In justified cases, certificates may be issued as PKCS10 files (certificates for the MQ Server).

Security of messages transmitted via the ESDK system is ensured by cryptographic methods based on PKI solutions and certificates. Electronic signature in message structure enables verification of message integrity and non-repudiation of the sender. Electronic signatures are generated for a data buffer including the main message as well as sender and recipient identifiers, message number and type, and message generation date and time. Only messages with a positively verified electronic signature are accepted for processing. Certificates are issued and managed using KDPW's existing PKI (Certification Authority). Certificates are issued by the Certification Authority under X.509 v.3 and electronic signatures are generated under PKCS7 with the RSA asymmetric algorithm using at least 1,024 bit keys. SWI Participants are authenticated and authorised for the ESDK message queue under TSL and certificates identifying the user in the system. To ensure data transmission security, communication between SWI Participant systems and KDPW via ESDK is via VPN channels (IPSec protocol) and/or TLS channels in MQ software between KDPW and the SWI Participant. IPSec protocol ensures SWI Participant authentication and guarantees data confidentiality and integrity in the transport layer. VPN channels terminate on KDPW side at a VPN concentrator which is an access node, and on the SWI Participant's side at any network device supporting IPSec protocol (router, VPN box, firewall) or directly at a PC with necessary client software (Cisco VPN Client).

Appendix 2 to the SWI Rules

(Version for KDPW participants and KDPW_CCP participants)

Power of attorney
to present declarations of intent via the Information Exchange System

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 6 sub-paragraph 1 point 1 of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... *(Principal's (company) name)* ("**SWI Participant**"), I/we the undersigned acting on behalf of the SWI Participant hereby grant to Mr/Ms ..... *(proxy's full name)*, PESEL identification number / passport number* ....., born on* ..... *(DD-MM-YYYY)*, this power of attorney to present declarations of intent on behalf of the SWI Participant via ESDI/WEB, ESDK*, and authorise the Proxy named above to present, with binding effect on the SWI Participant, to KDPW and to KDPW_CCP S.A.* other information and documents which may or should be transmitted in electronic form under regulations issued by KDPW or KDPW_CCP S.A.,* to request the generation of new security measures assigned to the SWI Participant according to § 15 sub-paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for ESDI/WEB, ESDK*, the security measures for the communication channel between KDPW and the SWI Participant and the security measures for test versions of the electronic communication systems.

.....

.....
Full names of persons
authorised to represent the Principal

* - delete if inapplicable. For a Polish national, enter the PESEL number; for a foreign national, enter the passport number and the date of birth.

Appendix 2 to the SWI Rules

(Version for Pension Fund Companies and Open Pension Funds)

Power of attorney
to present declarations of intent via the Information Exchange System

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 6 sub-paragraph 1 point 1 of the SWI Rules and the Agreement, concerning presentation of declarations and transmission of documents in electronic form, between Krajowy Depozyt Papierów Wartościowych S.A. and ..... (Principal's (company) name) ("SWI Participant") ("SWI Agreement"), I/we the undersigned acting on behalf of the SWI Participant hereby grant to Mr/Ms ..... (proxy's full name), PESEL identification number / passport number* ....., born on* ..... (DD-MMYYYY), this power of attorney to present to and to receive from KDPW and KDPW_CCP, on behalf of and with binding effect on the SWI Participant, other information and documents, which in accordance with KDPW or KDPW_CCP regulations may be, or need to be sent in electronic form, to request the generation of new security measures assigned to the SWI Participant according to the provisions of § 15 sub- paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for ESDI/WEB, ESDK*, the security measures to protect the communication channel between KDPW and the SWI Participant, and the security measures for test versions of electronic communication systems.

.....

.....
Full names of persons
authorised to represent the Principal

* - delete if inapplicable. For a Polish national, enter the PESEL number; for a foreign national, enter the passport number and the date of birth.

Appendix 2a to the SWI Rules

(Version for KDPW participants and KDPW_CCP participants)

Power of attorney
to present declarations of intent via the Information Exchange System
(template used to grant a power of attorney to another entity)

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 6 sub-paragraph 1 point 1 and § 17 sub-paragraph 1 of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... (Principal's (company) name) ("SWI Participant"), I/we the undersigned acting on behalf of the SWI Participant hereby grant to ..... (proxy's name) with its seat in ....., address: ....., entry in the court register number: ....., this power of attorney to present and receive, on behalf of and with binding effect on the SWI Participant, declarations of intent via ESDI/WEB, ESDK*, and authorise the Proxy named above to present, with binding effect on the SWI Participant, to KDPW and to KDPW_CCP S.A.* other information and documents which may or should be transmitted in electronic form under regulations issued by KDPW or KDPW_CCP S.A.,* to request the generation of new security measures assigned to the SWI Participant according to § 15 sub-paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for ESDI/WEB, ESDK*, the security measures for the communication channel between KDPW and the SWI Participant and the security measures for test versions of the electronic communication systems.

The proxy is authorised to authorise further proxies on behalf of the SWI Participant.

.....

.....
Full names of persons
authorised to represent the Principal

* - delete if inapplicable.

KDPW

Appendix 2a to the SWI Rules

(Version for Pension Fund Companies and Open Pension Funds)

Power of attorney
to present declarations of intent via the Information Exchange System
(template used to grant a power of attorney to another entity)

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 6 sub-paragraph 1 point 1 and § 17 sub-paragraph 1 of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... (Principal's (company) name) ("SWI Participant") ("SWI Agreement"), I/we the undersigned acting on behalf of the SWI Participant hereby grant to ..... (proxy's name) with its seat in ....., address: ....., entry in the court register number: ....., this power of attorney to present and receive, on behalf of and with binding effect on the SWI Participant, declarations and information referred to in § 1 sub-paragraph 3 of the SWI Agreement via ESDI/WEB, to request the generation of new security measures assigned to the SWI Participant according to § 15 sub-paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for ESDI/WEB and the security measures for test versions of ESDI/WEB.

The proxy is authorised to authorise further proxies on behalf of the SWI Participant.

.....

.....
Full names of persons

authorised to represent the Principal

KDPW

Appendix 2b to the SWI Rules

(Version for KDPW participants and KDPW_CCP participants)

Power of attorney
to present declarations of intent via the Information Exchange System
(template used to authorise a further proxy)

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 6 sub-paragraph 1 point 1 and § 17 sub-paragraph 1 and 2 of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... (Principal's (company) name) ("SWI Participant"), I/we the undersigned acting on the basis of a power of attorney granted by the SWI Participant on ....., with the right to authorise further proxies of the SWI Participant, hereby grant to Mr/Ms ..... (proxy's full name), PESEL identification number / passport number* ....., born on* ..... (DD-MM-YYYY), this further power of attorney to present and receive, on behalf of and with binding effect on the SWI Participant, declarations of intent via ESDI/WEB, ESDK*, and authorise the Proxy named above to present, with binding effect on the SWI Participant, to KDPW and to KDPW_CCP S.A.* other information and documents which may or should be transmitted in electronic form under regulations issued by KDPW or KDPW_CCP S.A.,* to request the generation of new security measures assigned to the SWI Participant according to § 15 sub-paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for the communication channel between KDPW and the SWI Participant and the security measures for test versions of the electronic communication systems.

.....

.....
Full names of persons
authorised to represent the Principal

* - delete if inapplicable. For a Polish national, enter the PESEL number; for a foreign national, enter the passport number and the date of birth.

KDPW

Appendix 2b to the SWI Rules

(Version for Pension Fund Companies and Open Pension Funds)

Power of attorney
to present declarations of intent via the Information Exchange System
(template used to authorise a further proxy)

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 6 sub-paragraph 1 point 1 and § 17 sub-paragraph 1 and 2 of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... (Principal's (company) name) ("SWI Participant") ("SWI Agreement"), I/we the undersigned acting on the basis of a power of attorney granted by the SWI Participant on ....., with the right to authorise further proxies of the SWI Participant, hereby grant to Mr/Ms ..... (proxy's full name), PESEL identification number / passport number* ....., born on* ..... (DD-MM-YYYY), this further power of attorney to present and receive, on behalf of and with binding effect on the SWI Participant, declarations and information referred to in § 1 sub-paragraph 3 of the SWI Agreement via ESDI/WEB, to request the generation of new security measures assigned to the SWI Participant according to § 15 sub-paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for ESDI/WEB and the security measures for test versions of ESDI/WEB.

.....

.....
Full names of persons
authorised to represent the Principal

* - delete if inapplicable. For a Polish national, enter the PESEL number; for a foreign national, enter the passport number and the date of birth.

KDPW

Appendix 2c to the SWI Rules

(Version for Account Operators)

Power of attorney
to present declarations of intent via the Information Exchange System

.....
Place and date

.....
Institution identifier

In connection with the provisions of § 17a sub-paragraph 2 and 3(a) of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... (name of the Account Operator) ("SWI Participant") ("SWI Agreement"), concluded by SWI Participant as Account Operator appointed by ..... ((company) name of the participant of the depository system who has appointed the SWI Participant as Account Operator) ("Represented Participant"), I/we the undersigned acting on the basis of a power of attorney granted by the Represented Participant to the SWI Participant on ....., with the right to authorise further proxies, hereby grant to Mr/Ms ..... (proxy's full name), PESEL identification number / passport number* ....., born on* ..... (DD-MM-YYYY), this further power of attorney to present and receive, on behalf of and with binding effect on the Represented Participant, in relations with Krajowy Depozyt Papierów Wartościowych S.A. and with participants of the depository system operated by Krajowy Depozyt Papierów Wartościowych S.A., declarations and information, including declarations of intent referred to in § 1 sub-paragraph 6 of the SWI Agreement, via ESDI/WEB, ESDK*, to request the generation of new security measures according to § 15 sub-paragraph 3 and 4 of the SWI Rules, and to collect from KDPW the security measures for ESDI/WEB, ESDK*, the security measures for the communication channel between KDPW and the SWI Participant, and the security measures for test versions of the electronic communication systems.

.....

.....
Full names of persons
authorised to represent the Principal

* - delete if inapplicable. For a Polish national, enter the PESEL number; for a foreign national, enter the passport number and the date of birth.

KDPW

Appendix 3 to the SWI Rules

CERTIFICATION FORM

	SUBSCRIBER		
A	**PERSONAL DATA**		
	A1. First name		A2. Last name
	A3. Country code	A4. Nationality	A5. PESEL[1] / Date of birth [2]
	A6. Identity document ☐ ID card [1] ☐ passport [2]		A7. Series and number
	CONTACT DETAILS		
	A8. E-mail		A9. Telephone

	CERTIFICATION DATA		
B	B1. Environment: ☐ production ☐ test	B2. Application ☐ - ESDI/WEB system certificate ☐ - ESDK system certificate	B3. Institution identifier
	B4. SWI Participant name		

	SUBSCRIBER'S DECLARATION AND SIGNATURE
C	C1[3]. I hereby declare that:[4] ☐ I am a politically exposed person.[5] ☐ I am a family member[6] of a politically exposed person. ☐ I am a close associate[7] of a politically exposed person. ☐ I am not a politically exposed person or a family member or close associate of a politically exposed person. I am aware of criminal liability for false declarations.
	C2. Date and signature of the subscriber.

[1] For a Polish national, enter the PESEL number.
[2] For a foreign national, enter the date of birth.
[3] Section C1 is to be completed only if section B3 includes an institution identifier of a direct participant with one of the following types of activity: 07, 09, 19, or 20. Otherwise, section C1 is to remain empty.
[4] Check the correct box
[5] A Politically Exposed Person shall mean a person within the meaning of Art. 2 subpara. 2 point 11 a-j of the Law of 1 March 2018 on Anti-money laundering and anti-terrorism financing (i.e. Dz. U. (Journal of Laws) 2022 item 593), who holds, or has over the past 12 months held the status of a person indicated in the abovementioned Art. 2 subpara. 2 point 11 a-j of the aforementioned Law.
[6] Family members of politically exposed persons shall mean a person within the meaning of Art. 2 subpara. 2 point 3 a-c of the Law of 1 March 2018 on Anti-money laundering and anti-terrorism financing (i.e. Dz. U. (Journal of Laws) 2022 item 593).
[7] Close associates of politically exposed persons shall mean a person within the meaning of Art. 2 subpara. 2 point 12 a and b of the Law of 1 March 2018 on Anti-money laundering and anti-terrorism financing (i.e. Dz. U. (Journal of Laws) 2022 item 593).

KDPW

INFORMATION FOR SUBSCRIBERS

The controller of your personal data is the Central Securities Depository of Poland (Krajowy Depozyt Papierów Wartościowych S.A. – KDPW) with is corporate address in Warsaw (00-498) at ul. Książęca 4. KDPW may be contacted via e-mail: kdpw@kdpw.pl or in writing at the above address.

Legal basis and purpose of processing:
- legitimate interests pursued by KDPW S.A., which require the identification of you as a person sending information to KDPW S.A. on behalf of an entity which has designated you as a proxy/further proxy authorised to submit on its behalf instructions via ESDI/WEB or ESDK, in accordance with the provisions of the Agreement concerning presentation of declarations and submission of documents in electronic form and in order to ensure the security of trading and other responsibilities carried out by KDPW S.A., enforcing or defending potential claims or rights of KDPW S.A. or an entity which has signed an agreement or entered into another legal relationship with KDPW S.A.;
- compliance with legal obligations – such obligations derive from the provisions of anti-money laundering legislation or the securities law.

We may pass on your personal data to entities or agencies which are authorised by law to obtain them.

Your personal data will be stored for a duration of no longer than 10 years from the date of the termination of participation in the SWI system of the entity which designated you as proxy/further proxy authorised to submit on its behalf instructions via ESDI/WEB or ESDK, in accordance with the provisions of the Agreement concerning presentation of declarations and submission of documents in electronic form. In the event of any dispute, judicial proceedings, or other legal action, the duration of the storage of the personal data will be determined from the date of the lawful termination of the dispute and in the event of several legal actions taking place – the date of the lawful termination of the last of these legal actions, irrespective of the manner of termination, unless legal rules indicate a longer period for the storage of data, or a longer limitation period for the claims or the rights on which the legal action is based.

You have the right of access to your personal data, the right to rectification of such data where it is factually incorrect and additionally, where provision has been made in national law, the right to erasure of such data and the right to restriction of processing. You have the right to object to the processing of your personal data. You have the right to portability of your data. You have the right to lodge a complaint with a supervisory authority regarding the processing of your personal data.

Providing your personal data is a voluntary action and it is derived from the existing legal relationship between KDPW S.A. and the entity which has designated you as its proxy/further proxy authorised to submit on its behalf instructions via ESDI/WEB or ESDK in accordance with the provisions of the Agreement concerning presentation of declarations and submission of documents in electronic form. Failure to provide your personal data will prevent you from being issued a certificate enabling the transmission of information via ESDI/WEB and ESDK.

Your personal data will not be used for automated decision-making, including profiling, except where profiling may be related to the fulfilment of requirements derived from the law, for instance, the requirement to assess the risk of money laundering and financing of terrorism.

	I hereby represent that I have read the information above.

D	D1. Date and signature of the subscriber.

KDPW

Appendix 4 to the SWI Rules

Declaration of authorisation of a private cryptographic key

.....

Place and date

.....

Institution identifier

I the undersigned ....., address of residence: ..... (city) ..... (street), ID / passport* series ..... number ..... issued by ....., valid until ……., hereby represent that:

1. I accept the private cryptographic key handed to me according to the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... *(Principal's (company) name)* ("**SWI Participant**"), corresponding to the certificate with the Common Name: ....., as my personal signature which identifies me to the same extent as my hand-written signature;

2. I accept all documents transmitted to Krajowy Depozyt Papierów Wartościowych S.A. via ESDI/WEB, ESDK*, as documents signed by me, and all declarations contained therein as presented by me on behalf of the SWI Participant, provided that they are positively verified as authorised messages;

3. I shall use the above mentioned private cryptographic key handed to me only to present declarations of intent on behalf of the SWI Participant transmitted via the ESDI/WEB, ESDK* system.

.....

Signature of the person presenting the declaration

* - delete if inapplicable

KDPW

Appendix 4a to the SWI Rules

(Version for Account Operators)

Declaration of authorisation of a private cryptographic key

.....

Place and date

.....

Institution identifier

I the undersigned ....., address of residence: ..... (city) ..... (street), ID/passport* series ..... number ..... issued by ....., valid until ....., hereby represent that:

1) acting as a further proxy of ..... *(name of the participant of the depository system who is not a SWI Participant and is represented by the Account Operator)* ("**Represented Participant**"), I accept the private cryptographic key handed to me according to the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form between Krajowy Depozyt Papierów Wartościowych S.A. and ..... *(name of the Account Operator)*, corresponding to the certificate with the Common Name: ....., as my personal signature which identifies me to the same extent as my hand-written signature;

2) I accept all documents transmitted to Krajowy Depozyt Papierów Wartościowych S.A. via ESDI/WEB, ESDK*, as documents sent by me, and all declarations contained therein as presented by me on behalf of the Represented Participant, subject to their provided that they are positively verified as authorised messages;

3) I shall use the above mentioned private cryptographic key handed to me only to present declarations of intent on behalf of the Represented Participant sent via the ESDI/WEB, ESDK* system.

.....

Signature of the person presenting the declaration

KDPW

* - delete if inapplicable

Appendix 5
to the SWI Rules

Identification details of the person authorised to transmit information via the SWIFT Message Processing System

In connection with § 19 sub-paragraph 1 of the SWI Rules and the Agreement concerning presentation of declarations and transmission of documents in electronic form with Krajowy Depozyt Papierów Wartościowych S.A., I/we the undersigned acting on behalf of ……....., with its registered office in ....., address: ....., entry in the official register number: …… , institution identifier : …… ("**SWI Participant**"), hereby represent that the following person:

PERSONAL DATA		
1. First name		2. Last name
3. Country code	4. Nationality	5. PESEL[1] / Date of birth [2]
6. Copy of an identity document authenticated by a notary public ☐ ID card [1] ☐ passport [2]		7. Series and number
CONTACT DETAILS		
8. E-mail		9. Telephone

is authorised to make on our behalf declarations of intent via the SWIFT Message Processing System and will send to KDPW all documents marked with BIC …… identifying the SWI Participant in the SWIFT network.
In case of revocation or expiration of the authorisation given to the person named above or in case of any change of the person through whom we will made declarations and transmit documents to KDPW via the SWIFT Message Processing System, we shall immediately present to KDPW a declaration as above naming a new person through whom we will operate in the SWIFT Message Processing System.

…… ……
Full names of persons authorised to represent the SWI Participant

[1] For a Polish national, enter the PESEL number.
[2] For a foreign national, enter the date of birth.

The controller of your personal data is the Central Securities Depository of Poland (Krajowy Depozyt Papierów Wartościowych S.A. – KDPW) with is corporate address in Warsaw (00-498) at ul. Książęca 4. KDPW may be contacted via e-mail: kdpw@kdpw.pl or in writing at the above address.

Legal basis and purpose of processing:
- legitimate interests pursued by KDPW S.A., which require the identification of you as a person sending information to KDPW S.A. on behalf of an entity which has indicated you as a person authorised to submit on its behalf instructions via the SWIFT Message Processing System, in accordance with the provisions of the Agreement concerning presentation of declarations and submission of documents in electronic form and in order to ensure the security of trading and other responsibilities carried out by KDPW, enforcing or defending potential claims or rights of KDPW S.A. or an entity which has signed an agreement or entered into another legal relationship with KDPW S.A.;
- compliance with legal obligations – such obligations derive from the provisions of anti-money laundering legislation or the financial instruments trading law.

We may pass on your personal data to entities or agencies which are authorised by law to obtain them. Your personal data will be stored for a duration of no longer than 10 years from the date of the termination of participation in the SWI system of the entity which designated you as proxy/further proxy authorised to submit on its behalf instructions via the SWIFT Message Processing System, in accordance with the provisions of the Agreement concerning presentation of declarations and submission of documents in electronic form. In the event of any dispute, judicial proceedings, or other legal action, the duration of the storage of the personal data will be determined from the date of the lawful termination of the dispute and in the event of several legal actions taking place – the date of the lawful termination of the last of these legal actions, irrespective of the manner of termination, unless legal rules indicate a longer period for the storage of data, or a longer limitation period for the claims or the right on which the legal action is based.

You have the right of access to your personal data, the right to rectification of such data where it is factually incorrect and additionally, where provision has been made in national law, the right to erasure of such data and the right to restriction of processing. You have the right to object to the processing of your personal data. You have the right to portability of your data.

You have the right to lodge a complaint with a supervisory authority regarding the processing of your personal data.

Providing your personal data is a voluntary action and it is derived from the existing legal relationship between KDPW S.A. and the entity which has indicated you as the person authorised to submit on its behalf instructions via the SWIFT Message Processing System in accordance with the provisions of the Agreement concerning presentation of declarations and submission of documents in electronic form. Failure to provide your personal data will prevent you from being sent information via the SWIFT Message Processing System on behalf of the aforementioned entity. Your personal data will not be used for automated decision-making, including profiling, except where profiling may be related to compliance with legal requirements, e.g., to rate the risk of money laundering or the financing of terrorism.

.....
Date and signature of the person authorised by the SWI Participant

ADDITIONAL DECLARATIONS OF THE PERSON AUTHORISED BY THE SWI PARTICIPANT[10]
I hereby declare that:[11] ☐ I am a politically exposed person.[12] ☐ I am a family member[13] of a politically exposed person. ☐ I am a close associate[14] of a politically exposed person. ☐ I am not a politically exposed person or a family member or close associate of a politically exposed person.
I am aware of criminal liability for false declarations.
Date and signature of the of the person authorised by the SWI Participant.

[10] The additional declaration is only required from a person authorised by an SWI Participant which is a direct participant with one of the following activity status types: 07, 09, 19 or 20. Persons authorised by other SWI Participants are not required to make the declaration

[11] Check the correct box.

[12] A Politically Exposed Person shall mean a person within the meaning of Art. 2 subpara. 2 point 11 a-j of the Law of 1 March 2018 on Anti-money laundering and anti-terrorism financing (i.e. Dz. U. (Journal of Laws) 2022 item 593), who holds, or has over the past 12 months held the status of a person indicated in the abovementioned Art. 2 subpara. 2 point 11 a-j of the aforementioned Law.

[13] Family members of politically exposed persons shall mean a person within the meaning of Art. 2 subpara. 2 point 3 a-c of the Law of 1 March 2018 on Anti-money laundering and anti-terrorism financing (i.e. Dz. U. (Journal of Laws) 2022 item 593).

[14] Close associates of politically exposed persons shall mean a person within the meaning of Art. 2 subpara. 2 point 12 a and b of the Law of 1 March 2018 on Anti-money laundering and anti-terrorism financing (i.e. Dz. U. (Journal of Laws) 2022 item 593).

Terms of use of the Information Exchange System for communication between the SWI Participant and KDPW_CCP S.A.

1. The following terms used in the SWI Rules shall have the following meaning:

    1) **KDPW_CCP regulations** – means the regulations approved by the Supervisory Board of KDPW_CCP S.A. and resolutions of the Management Board of KDPW_CCP S.A. issued under such regulations, which lay down the rules of KDPW_CCP S.A.'s clearing of transactions executed in financial instruments trading;

    2) **CCP documents** – means documents containing information and declarations, including declarations of intent, originating from the SWI Participant or from KDPW_CCP S.A., which under KDPW_CCP regulations may or should be transmitted in electronic form between the SWI Participant and KDPW_CCP S.A.;

    3) **CCP system documents** – means such CCP documents which are generated directly from the IT system used by KDPW_CCP S.A. to operate the clearing of transactions or recorded directly in that IT system, including without limitation IR daily reports and position transfer orders within the meaning of KDPW_CCP regulations.

2. KDPW approves the SWI Participant's use of the Information Exchange System for communication between the SWI Participant and KDPW_CCP S.A. with respect to CCP system documents and on the terms laid down in this Appendix.

3. CCP documents shall be sent by the SWI Participant to KDPW_CCP S.A. and CCP system documents shall be sent by KDPW_CCP S.A. to the SWI Participant via KDPW.

4. Subject to paragraph 5, only CCP system documents may be transmitted via ESDK and the SWIFT Message Processing System, whereas only such SWIFT messages may be transmitted via the SWIFT Message Processing System which are indicated on the KDPW website as approved for transmission via the system. Any CCP documents may be transmitted via ESDI/WEB.

5. Transmission of CCP documents by the SWI Participant to KDPW_CCP S.A. via the SWIFT Message Processing System shall require prior activation of such electronic communication system between the SWI Participant and KDPW.

6. CCP system documents or other CCP documents addressed to KDPW_CCP S.A. shall be sent by the SWI Participant to KDPW pursuant to the provisions of the SWI Agreement and the SWI Rules in the mode relevant to the transmission of system documents or other documents, respectively, by the SWI Participant to KDPW, provided that:

    1) CCP system documents in XML format sent to KDPW via ESDK shall contain the identifier of KDPW_CCP S.A. in the header and in the recipient field;

    2) CCP system documents in relevant SWIFT message format shall contain the identifier of KDPW_CCP S.A. in the recipient field according to the documentation available on the KDPW website;

3) other CCP documents including CCP system documents sent to KDPW via ESDI/WEB shall name KDPW_CCP S.A. as the recipient in their content.

7. The provisions of § 8 sub-paragraphs 1-3, § 9 sub-paragraph 1, § 15 sub-paragraph 2, § 16 sub-paragraphs 2 and 4, § 19 sub-paragraphs 3-8, shall apply accordingly to CCP documents sent by the SWI Participant and addressed to KDPW_CCP S.A., subject to the other provisions of this Appendix.

8. Verification of authenticity of messages contained in CCP system documents sent by the SWI Participant shall be performed by KDPW, which in the event of negative verification of message authenticity shall notify the SWI Participant.

9. CCP documents originating from the SWI Participant shall be made available to KDPW_CCP S.A. immediately upon their delivery to KDPW in accordance with this Appendix provided that the verification of message authenticity is not negative and for CCP system documents in XML format sent via ESDK additionally provided that they comply with the requirement set out in sub-paragraph 6 point 1. KDPW shall not be required to, but may, make available to KDPW_CCP S.A. CCP documents originating from the SWI Participant referred to in sub-paragraph 6 points 2 and 3 unless they comply with the requirements set out therein.

10. By delivering a CCP document to KDPW, the SWI Participant authorises KDPW:

    1) to make such document available to KDPW_CCP S.A.;

    2) for CCP documents referred to in sub-paragraph 6 points 2 and 3, to review the content of the document in order to determine whether KDPW_CCP S.A. is its recipient.

11. CCP system documents or other CCP documents originating from KDPW_CCP S.A. and addressed to the SWI Participant shall be sent by KDPW to the SWI Participant pursuant to the provisions of the Agreement in the mode relevant to the transmission of system documents or other documents, respectively, by KDPW, provided that:

    1) CCP system documents in XML format sent to the SWI Participant via ESDK shall contain the identifier of KDPW_CCP S.A. in the header and in the sender field;

    2) CCP system documents in relevant SWIFT message format shall contain the identifier of KDPW_CCP S.A. in the sender field according to the documentation available on the KDPW website;

    3) other CCP documents including CCP system documents sent to the SWI Participant via ESDI/WEB shall name KDPW_CCP S.A. as the sender in their content.

12. The provisions of § 8 sub-paragraphs 1-3, § 9 sub-paragraph 1, § 15 sub-paragraph 2, § 16 sub-paragraphs 2 and 4, § 19 sub-paragraphs 3 and 7-8, shall apply accordingly to CCP documents addressed to the SWI Participant and sent by KDPW_CCP S.A. via KDPW, subject to the other provisions of this Appendix.

13. CCP documents originating from KDPW_CCP S.A. and addressed to the SWI Participant shall be sent to the SWI Participant immediately upon their receipt by KDPW.

14. Declarations of intent and information contained in CCP documents authenticated with the SWI Participant's certificate or including the BIC identifying the SWI Participant in the SWIFT network shall not be considered declarations of intent submitted by the SWI Participant to KDPW or information addressed by the SWI Participant to KDPW.

15. Attaching KDPW's electronic signature or the BIC identifying KDPW in the SWIFT network to a CCP document shall be considered by the Parties only to be confirmation given by KDPW that the document originates from KDPW_CCP S.A. Under no circumstances shall such document be considered a document containing an own declaration of KDPW or information addressed by KDPW to the SWI Participant.

16. The SWI Participant represents that during its participation in the transaction clearing system operated by KDPW_CCP S.A., persons authorised by it to present on its behalf declarations of intent to KDPW or to send documents to KDPW via ESDI/WEB, ESDK or the SWIFT Message Processing System shall be authorised to present on its behalf, via the same electronic communication system or systems, declarations of intent and other declarations and information which may be contained in CCP documents addressed by the SWI Participant to KDPW_CCP S.A.