# CONDITIONS OF DATA PROCESSING IN CDCP

EXECUTORY DECREE No.1 TO THE RULES OF OPERATION

CENTRÁLNY DEPOZITÁR CENNÝCH PAPIEROV SR, A.S.

## Article 1
## Introductory provisions

1.1 This Executory Decree is issued in compliance with the Article 3 par. 3.1 part VI – „Final provisions“ of the Rules of Operation and it shall set the conditions and rules for processing of data in Centrálny depozitár cenných papierov SR, a.s. (further referred to as the “central depository” or “CDCP”).

1.2 Specified conditions are binding for all authorised persons to whom services are provided by CDCP.

1.3 Fulfilling of specified conditions is supervised by appointed employees of CDCP.

1.4 In case the following expressions are used in next provisions of this Executory Decree, they have a below stated meaning:

a) „security“ - security/securities;

b) „IT“ – information technologies;

c) „IT user“ – employee representing authorised person, whereas the employee is skilled to execute procedures available via used information technologies;

d) „Act“ – the Act No.566/2001 Coll. on Securities and Investment Services and on amendments and supplements to certain laws;

e) „production system of CDCP“ – software and data equipment of CDCP created to facilitate execution of requests and obligations arising from the Act;

f) „authorised person“ – person specified in the Article 6 of part „Introductory provisions” of the Rules of Operation;

g) „protocol“ – document in written form declaring taking and hand over of data in electronic form;

h) „CA“ – Approved Certification Authority that was granted the licence to issue certificates;

i) „APV“ – application software.

## Article 2
## Method of connection to CDCP

2.1 Following methods of connection to the production system are available for the authorised persons:

a) direct connection – on-line via client application;

b) direct connection – on-line via swift communication system;

c) indirect connection – off-line (data medium etc.).

2.2 In case the direct connection is not accessible, the authorised person is allowed to use emergency mode based on agreement with CDCP whereas indirect connection is used in the emergency mode;

2.3 There are two options available in the emergency mode:

a) backup workplace of CDCP which is equipped by “anonymous” PC with internal connection to the APV of CDCP’s production system, i.e. authorised person shall bring input data records of services on a data medium, initialization data for the client application, and the certificate in respective form;

b) authorised person shall appear at dedicated workplace in CDCP where the person shall be allowed to connect its configured mobile device (notebook, etc.) to the production system.

2.4 Operation hours of the production system are laid down by the Board of Directors of CDCP. CDCP shall publish the information on operation hours on its web site www.cdcp.sk.

2.5 Format and structure of input and output files must comply with specification in respective version of APV of CDCP's production system.

2.6 Input files are considered to be received by the central depository if services contained in the files are confirmed by posting into archive of the CDCP's production system.

2.7 APV facilitating conversion of the issuer's registry balance statement output files are available at CDCP's web page from.

2.8 Authorised persons shall connect to the CDCP's production system in emergency mode pursuant to the previous indent under supervision of appointed employee of CDCP.

## Article 3
## Direct connection via client application

3.1 Authorised person who execute data exchange with CDCP via communication line (internet or telecommunication line) is obliged to obtain the telecommunication line at its own expenses. Technical options of connection must be negotiated with appointed employee of CDCP before application for this method of communication is submitted.

## Article 4
## Direct connection via SWIFT communication system

4.1 For description of data exchange between authorised person and CDCP via SWIFT communication system refer to the Executory Decree No.6.

## Article 5
## Indirect connection

5.1 Authorised person shall bring, on a data medium, the application data in "open" form (i.e. not encrypted), and it shall processed at dedicated workplace in CDCP, whereas a certificate of the workplace will be used. After processing the data it shall be handed over to the authorised person in open form. Access of the authorised person may carried out via data medium (CD-ROM, diskette 3.5″, USB-key).

5.2 Input files are taken from the authorised person, and output files are handed over to the authorised person during operation hours at dedicated taking/handing over point, except for special operation breaks. Takeover report for both parties is always issued at the moment of taking/handing over of data.

5.3 Takeover report must be attached to each complain of CDCP services related to processing of input file handed over at dedicated taking/handing over point.

5.4 CDCP employee at taking/handing over point is allowed to decide on cancellation of taking over/uploading of input files 30 minutes before termination of operation hours in case undertaking such step is required for finalisation of other activities in due form.

## Article 6
## Sending of data

6.1 When performing duties arising from claims and laws, CDCP is sending data:

a) electronically, encrypted with certificate and in agreed form;

b) via post at valid CDCP form;

c) in form of SWIFT messages via SWIFT communication system.

## Article 7

## Data registration and storage

7.1 CDCP shall administer a complete time-sequenced registry (archive) concerning bilateral data exchange with authorised persons.

7.2 CDCP recommends administering the registry pursuant to previous item also to authorised persons.

7.3 Entry in CDCP archive, or SWIFT, is predominant when resolving possible complains.

## Article 8

## Essential configuration of authorised person for connection with CDCP via client application

8.1 Authorised person (including applicant for CDCP membership) must meet requirements specified in this Article.

8.2 Authorised person is obliged to dedicate minimum 2 PC stations (hereinafter only “node”) with minimal configuration:

a) processor not less than Intel Pentium 42 GHz (or performance equivalent), memory 512 MB RAM,

b) Hard disc with minimum capacity 20 GB,

c) CD ROM or DVD ROM drive,

d) diskette drive 3,5“.

8.3 Dedicated node must be equipped with following software at least:

a) operation system Microsoft Windows 2000 Professional, Windows XP (also Linux, or Unix are allowed for client application of the registry module) with the latest service pack and critical updates installed,

b) .NET Framework 1.1. with the latest service pack and critical updates installed,

c) Web Services Enhancements 1.0 SP 1 or higher,

d) Microsoft Internet Explorer 6.0 or higher, eventually other equivalent product;

e) installed network support for TCP/IP, internet connection.

8.4 Authorised person is obliged to install SW for communication with CDCP in the nodes. To assure the installation, CDCP shall provide the authorised person with:

a) current version of APV which is required for connection with CDCP,

b) current structure specification and format of input/output records of CDCP services the authorised person has right to according to the agreement with the authorised person.

8.5 The authorised person must procure:

a) employees with valid „Certificate of Expertise“ issued by CDCP;

b) functional certificate/-s for employees as specified in item a), issued by a certification authority approved by CDCP,

c) registration of public keys in the CDCP’s production system for employees specified in item a);

d) take-over of CDCP’s public keys and their registration to the nodes of the authorised person.

8.6 CDCP recommends consulting all possible changes in setup of the node with dedicated employees of CDCP.

## Article 9
## Organisation of operation

9.1 Only persons who passed a professional examination pursuant to relevant provisions of the Rules of Operation – part “Rules of Membership”, are allowed to operate APV of the central depository.

9.2 CDCP shall provide following trainings for the authorised person:

a) Operation/Administration Training for the client application;

b) APV User Training in order to obtain „Certificate of Expertise“ (free of charge for 10 persons).

9.3 APV User Training attendee will gain knowledge needed to pass practical part of an examination to prove/demonstrate expertise pursuant to relevant provisions of the Rules of Operation – part “Rules of Membership”.

9.4 In order to establish an environment and ensure operation, CDCP shall provide the authorised person with the client application and actual APV documentation (CDCP web page), which is required for installation and use of production system services.

9.5 Data exchange runs via f software tools which are handed over to the authorised person for utilization after signing an agreement and operation protocol. Description of hardware, software, communication and other conditions of their installation and utilization is part of provided software products.

9.6 Detected technical or other problems related to APV operation are reported by the authorised person via non-stop CDCP Hot-line service.

## Article 10
## Competence rules

10.1 CDCP shall appoint responsible employees who shall be competent to solve issues related to particular elements of APV – Registry module and Clearing and Settlement module (hereinafter only “ZaV”). Responsible employees (hereinafter only “guarantor”) shall provide for communication with appointed competent and responsible employee of the authorised person with regard to respective element of APV (hereinafter only “member’s guarantor”) and with users of the authorised person concerning use of respective APV elements.

10.2 CDCP guarantor for registry module provides for following activities:

a) co-ordination of activities related to operation of Registry modules;

b) participation on preparation, adherence and control of activity schedule of Registry module in interaction with ZaV module;

c) collection and co-ordination of suggestions from employees of the authorised person related to the Registry area and co-operation when solving problems related to ZaV module;

d) administering a list of contact persons at the authorised person, who are considered a counterpart;

e) administering a registry of handed over issues of the client application, documentation, trainings, employee’s rights and certificates, as per member;

f) co-ordination of changes and modifications required by CDCP and their delivery by application provider;

g) co-ordination of activities with other specialized departments at division of Information technologies and other divisions of CDCP;

h) organisation of testing, training and examination of professionals of authorised persons with regard to the Registry module;

i) participation at preparation of methodical documents, user manuals and other documents with regard to the Registry module;

j) co-operation in solving complains from the authorised persons;

k) solving of critical situations with regard to the Registry module.

10.3 CDCP guarantor for ZaV module provides for following activities:

a) co-ordination of activities related to operation of ZaV modules,

b) participation on preparation, adherence and control of activity schedule of ZaV modules in interaction with the Registry module and BIPS module;

c) collection and co-ordination of suggestions from employees of the authorised persons related to the ZaV area and co-operation when solving problems related to the Registry module and BIPS module;

d) administering of list of contact persons at the authorised person, who are considered a counterpart;

e) administering a registry o handed over issues of the client application, documentation, trainings, employee’s rights and certificates, as per authorised person;

f) co-ordination of changes and modifications required by CDCP and their delivery by application provider;

g) co-ordination of activities with other specialized departments at division of Information technologies and other divisions of CDCP;

h) organisation of testing, training and examination of professionals of authorised persons with regard to the ZaV module;

i) participation at preparation of methodical documents, user manuals related to the ZaV module;

j) co-operation in solving complains from the authorised person and solving of critical situations with regard to the ZaV module.

10.4 The authorised person is obliged to appoint responsible employee – guarantor on behalf of member, for each element of APV (Registry module and ZaV module) who shall solve operation issues related to particular element of APV with respective guarantor of CDCP

10.5 Guarantor on behalf of a member will ensure following activities:

a) collaboration with CDCP’s guarantor responsible for particular APV module;

b) co-ordination of activities of particular APV module in collaboration with respective guarantor of the central depository;

c) co-ordinates interaction of related special departments of the authorised person through CDCP’s guarantor;

d) co-ordinates testing and training of professionals of the authorised person with regard to respective APV module;

e) co-ordinates activities related to implementation of new issues of respective APV modules at the authorised person;

f) co-ordinates activities related to complains from the authorised person and keeps registry of complains on behalf of the authorised person;

g) co-ordinates activities related to placing of certificates – electronic signature.

10.6 CDCP's guarantors are keeping unified register of APV users on behalf of the authorised person as per respective APV module base on "User cards" which are available at the web page of CDCP (see in case of following activities: guarantor/user of operation APV module and user of testing APV module.)

10.7 User card declares rights and obligations of APV user acting on behalf of the authorised person, confirmed by the statutory body of the authorised person, that qualify user to perform services and activities specified in the user card. CDCP shall set up rights in respective APV module for involved user based on submitted extent of rights and obligations.

10.8 Two originals of the user card are issued, whereas one original is placed into CDCP's register and other original is placed into register of the authorised person. Services, or activities, for which given user is not authorised by the authorised person must be clearly identified as unauthorised.

10.9 APV user card includes following basic data:

a) name, surname, date of birth, domicile;

b) official position, contact details (e-mail, telephone, fax);

c) address of the authorised person;

d) specimen signature;

e) training in CDCP and confirmation of qualification to work with the production system;

f) extent of rights with regard to respective APV module (list of confirmed services permitted to perform),

g) signature of authorised person's statutory body representatives declaring consent with performance of above mentioned services by the employee.

## Article 11
## Safety criteria of connection via client application

11.1 Authorised person is obliged to use certificates issued by certificate authorities specified on CDCP web page, and is obliged to preserve the private keys in such manner so it is not possible to misuse them. In case the certificates issued by different certification authority are being used, it is necessary to arrange for testing mode with CDCP.

11.2 The authorised person (guarantor) shall hand over certificate public key of new employee (user) to specified employee of CDCP along with specification of extent of rights for CDCP services, which should be assigned to respective certificate and definition of environment (testing/operation system) in it which will be used.

11.3 The authorised person is obliged to assure adequate protection of its private key and data media on which the private key is saved. CDCP is not responsible for damages that occurred due to processing of authorised input data as result of improper use of private key of the authorised person.

11.4 In case there exists risk of private key misuse, the authorised person (guarantor) is obliged to contact dedicated CDCP's employee without delay and ask for immediate cancellation of given public key.

11.5 It is not possible to use the certificate adequately for data exchange for last 30 days of the certificate validity. It is allowed only to receive output records of APV services with such certificate during this time period.

## Article 12
## Duties of the authorised person at data protection

12.1 The authorised person, in order to protect data in the production system of CDCP, is obliged to:

a) protect the client application from eventual changes and modifications which would corrupt its functionality or would break protection of processed data;

b) assure that cryptographic tools intended for data and service protection were used only by authorised employees of the authorised person with valid "Certificate of Expertise";

c) assure that unauthorised persons may not misuse the cryptographic tools intended for data and service protection;

d) report discrediting of cryptographic tools intended for protection of data and services of CDCP's production system without delay and execute measures for preventing of unfavourable consequences;

e) not provide software products, documentation and information related to the CDCP's production system to unqualified persons or subjects without previous written consent of CDCP.

12.2 CDCP is not responsible for damages occurred due to breach of duties concerning data protection by the authorised person pursuant to the provisions of this Article.

## Article 13
## Utilisation of certificate for processing of list of securities owners

13.1 It is possible to use certificate encryption pursuant to Article 11, item 11.1 of this Executory Decree to create a list of securities owners. In case the certificate is to be used, relevant documents must be submitted to CDCP at least one month in advance.

13.2 The issuer is obliged to submit the certificate public key of the certificate authority to relevant workplace in CDCP (Section of Securities Issues) five working days before processing of the service in PEM format and on stipulated data medium.

13.3 The issuer is obliged to submit to CDCP a certificate with new validity one month before validity expiration of the certificate. In other case the services shall be processed without the certificate. In case the issuer shall decide on cancelation of the certificate before expiration of its validity, the issuer is obliged to inform CDCP, Section of Securities of this fact without delay.

13.4 For decryption, the issuer is obliged to use actual APV in order to process delivered list of securities owners. APV for decryption shall be handed over to the issuer by CDCP, at the Section of Securities Issues, on data medium, along with the user manual, after concluding an agreement.

13.5 Conditions for installation of APV for decryption are specified in the Article 8, items 8.2 and 8.3 indent a) of this Executory Decree. Eventual consultations with regard to use of APV shall provide the Section of Securities Issues.

13.6 The lists of securities owners are converted to XML format decryption. Structure of output records of services for issuer is indicated at CDCP web page /www.cdcp.sk/.

13.7 Data of the file containing list of securities owners are in code page ISO LATIN 2 (ISO-88592). It is recommended to consult possible requirements related to conversion to different code with the Section of Securities Issues.

## Article 14
## Final provisions

14.1 This Executory Decree to the Rules of Operation is valid upon approval by the Board of Directors of CDCP and shall enter into force on 1 December 2012 and from this date the Executory Decree No.1 as of 30 January 2007 shall cease its validity and force.

| | |
|---|---|
| Daniel Jóna<br>Chairman of the Board | Vladimír Gürtler<br>Vice-chairman of the Board |