BANK GPB INTERNATIONAL S.A.
MEMBER OF GAZPROMBANK GROUP

Terms and Conditions for Electronic Data Transmission

(“EDT Terms and Conditions”)

1. Scope of services

(1) Bank GPB International S.A. (the “Bank”) is available to its Customers (according to Clause 14 account holders and /or Customer Affiliate(s)), not being a consumer, for electronic data interchange, hereinafter referred to as “electronic data interchange” or “EDT”. EDT comprises placing payment orders (“orders”) and exchanging data (transmission of orders and download information).

(2) The Bank will notify the Customer of the types of services which the Customer may use within the framework of EDT. The use of EDT is subject to the disposal limits agreed with the Bank.

(3) EDT is available via the EBICS interface (Annexes 1a to 1c).

(4) The structure of data records and files for transmission of orders and download of information is described in the specifications for data formats (Annex 2).

(5) Accounts held at a financial institution which does not belong to the same group as the Bank (third-party bank) can only be admitted to the EDT service (the “EDT Service”) if the Bank receives sufficient written confirmation from the third-party bank that the Customer (i) has authorised the third-party bank, on the basis of respective account agreement(s) with the third-party bank, to carry out instructions forwarded by the Bank in accordance with the EDT Terms and Conditions and (ii) has concluded a separate agreement with the third-party bank in order to ensure that the Bank receives the account information for the account in question.

(6) The Customer agrees and accepts that, for any matters not expressly referred to in the present Terms and Conditions for Electronic Data Transmission, the General Terms and Conditions of the Bank and, where relevant, the Specific Terms and Conditions for Payment Services of the Bank shall apply.

2 Users and participants, identification and security media

(1) Orders can only be placed by the Customer or its authorised agents, via the EBICS interface. The Customer and authorised agents are hereinafter collectively named “Users”. To place orders with the Bank, each User requires individual identification media which must be activated by the Bank. The requirements for the identification media are defined in Annex 1a.

(2) In addition to its authorised representatives, the Customer may designate “technical subscribers” who are solely authorised to exchange data via the EBICS interface. Users and technical subscribers are hereinafter collectively referred to as “Subscribers”. To protect the data exchange, each Subscriber requires individual security media which must be activated by the Bank. The requirements for the security media are described in Annex 1a. Subscribers qualify as agents (“*mandataires*”) of the Customer within the meaning of Article 1984 of the Civil Code.

(3) Identification and security media are instruments that allow for an authentication within the meaning of the Luxembourg payment services legislation).

3 Procedural provisions

(1) The transmission procedure agreed between the Customer and the Bank shall be subject to the requirements described in Annex 1a, the requirements described in the documentation of the technical interfaces (Annex 1b) and the specifications for the data formats (Annex 2).

(2) The Customer is obliged to ensure that all Subscribers observe the EDT procedures and specifications.

(3) The data files are assigned according to the assignment and control; guidelines for the format used (Annex 2).

(4) The User must correctly state the account identification code (account number or IBAN) of the payee or the payer and – as far as required – the payments service provider identification code (bank sort code or BIC) of the payee‘s payments service provider or the payer‘s payments service provider (paying agent). The payment service providers involved in the settlement of the payment order are authorised to process the transaction exclusively on the basis of the account identification code and – if stated – the payments service provider identification code. Incorrect information may cause a payment to be misrouted and thus result in damage for the Customer. Any damages or losses which may arise therefrom shall be borne exclusively by the Customer.

(5) Prior to the transmission of the order data to the Bank, a record of the full contents of the files to be transmitted and of the data transmitted for the verification of identification must be prepared. Such record must be kept by the Customer for a minimum of 30 calendar days from the date of execution in such form that it can be made available to the Bank again at short notice on request, unless otherwise agreed.

(6) In addition, the Customer must generate an electronic protocol for each data exchange according to section 10 of the EBICS specification link (Annex 1b) and must file this protocol with its documents and make them available to the Bank upon request.

(7) To the extent the Bank provides the Customer with data on payment transactions which are not yet finally processed, such data shall be deemed to be only non-binding information. Such data will be specifically marked. However, other data may also at all times be amended by the Bank in order to *i.a.* correct errors.

As agreed with the Bank, order data transferred via EDT is to be authorised only by an electronic signature. Such order data shall be effective as an order for data submitted with an electronic signature:

- if all necessary electronic signatures of Users have been received via data communications within the agreed period of time, and
- if the electronic signatures can be successfully checked against the agreed keys.

4 Duties of care with respect to the legitimation media for the authorisation of orders

(1) Depending on the transmission procedure agreed with the Bank, the Customer is obliged to ensure that all Users comply with the legitimation procedures described in Annex 1a.

(2) The User may place orders by means of the legitimation media activated by the Bank. The Customer shall ensure that all Users take precautions that no third-party obtains possession of the User’s legitimation medium or gains knowledge of the password protecting it. This is because any third person who has obtained possession of the medium or a duplicate thereof can misuse the agreed services in conjunction with the corresponding password. The following shall be observed in particular to keep the legitimation media secret:

– the data legitimising the User may not be stored outside the legitimation media, for example on the computer’s hard disk,
– the legitimation medium must be kept safely after the end of the remote data transmission procedure,
– the password protecting the legitimation medium may not be written down or stored electronically,
– when entering the password, care must be taken to ensure that no other persons can steal it,
– the legitimation media must never be communicated to any other person, not even to relatives or trusted third parties, to the Bank, to the police or insurance services and more generally to any merchant and in particular by phone or online, and
– the Users should never let themselves get distracted during an operation including by third parties offering their help and to avoid entering their passcodes in front of them.

5 Duties of care for dealing with security media required for data exchange

With respect to the connection via EBICS, the Customer is obliged to ensure that all Subscribers comply with the security procedures described in Annex 1a.

Subscribers shall secure the data exchange by means of the security media activated by the Bank. The Customer is obliged to request each User to ensure that no third-party obtains possession of the security medium or is able to use it. In particular as regards to storage in a technical system, the Subscriber’s security medium must be stored in a technical environment which is protected against unauthorised access. This is because any third person who gains access to the security medium or a duplicate thereof may misuse the data exchange.

6 Suspension of legitimation and security media

(1) If the legitimation or security media are lost, become known to third-parties or misuse of such media is suspected, the Subscriber must immediately suspend EDT access or request the Bank to suspend the EDT access. Further details are stipulated in Annex 1a. The Subscribers can send the Bank a blocking notice at any time, using the contact details supplied separately if necessary.

(2) Outside the EDT process, the Customer may request suspension of a Subscriber’s legitimation and security media or the entire EDT access via the suspension facility provided by the Bank.

(3) The Bank will suspend the entire EDT access, if there is a reason to suspect that EDT access has been misused. The Bank will inform the Customer accordingly outside the EDT process. This suspension cannot be lifted using EDT technology.

7 Processing of incoming order data by the Bank

(1) The order data transmitted to the Bank by EDT are processed during the normal course of work.

(2) On the basis of the signatures generated by the Subscribers with the security media, the Bank will verify whether the sender is authorised to perform the data exchange. If this verification reveals any discrepancies, according to the discretionary assessment of the Bank, the Bank will not process the affected order data and will notify the Customer thereof.

(3) The Bank will verify the legitimation of the User(s) and the authorisation of the order data transmitted by the EDT on the basis of the electronic signatures produced by the User(s) within the legitimation media or the accompanying supporting note and shall check the correspondence between the order records and the provisions contained in Annex 2. If this verification reveals any discrepancies, according to the discretionary assessment of the Bank, the Bank will not process the affected order data and will notify

the Customer thereof. The Bank is entitled to delete order data not fully authorised after expiry of the time limit that is separately indicated by the Bank.

(4) If errors are revealed by the Bank's verification of files or data records, the Bank will provide information on the errors in the files or data records in the form it deems fit and notify the User thereof immediately. The Bank shall be authorised to exclude files or data records with errors from further processing at its discretion.

(5) The Bank will document these procedures (see Annex1a) and the forwarding of the orders for processing in the Customer protocol. The Customer in turn shall be obliged to retrieve the Customer report promptly and to keep himself / herself informed of the processing of the order. In the event of any discrepancies, the Customer should immediately contact the Bank.

8 Recall

(1) Before the authorisation of the order data, the Customer shall be entitled to recall the file. Individual order data can only be changed by recalling the whole file and placing the order again. The Bank can only accept a withdrawal if it is received in good time so that it can be taken into account in the course of the normal working procedures.

(2) The extent to which an order can be recalled depends on the relevant special conditions (notably the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank). Orders can only be recalled outside the EDT process. To do this, the Customer must inform the Bank of the individual details of the original order.

9 Processing orders

(1) The Bank will process the orders if all the following requirements for processing have been fulfilled:

- the order data transmitted by EDT has been authorised in accordance with Clause 3 (8),
- the defined data format must be complied with,
- the credit limit must not be exceeded,
- the processing requirements according to the special criteria in relation to the relevant order type are met (*i.a.* sufficient funds according to the provisions of the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank).

(2) If the conditions for processing outlined in sub-section 1 above are not fulfilled, the Bank will not process the order and will notify the Customer hereof through the agreed communication channel. As far as possible, the Bank will notify the Customer of the reasons and errors which caused the order not to be processed and the possible ways to correct these errors.

10 Security of the Customer's system

The Customer shall ensure that the systems used for the EDT are equally protected. The security requirements that are applicable relating to the EBICS process are described in Annex 1c.

11 Liability

11.1 The Bank's liability for an unauthorised EDT transaction and an unprocessed or incorrectly processed EDT transaction

The Bank's liability for an unauthorised and for an unprocessed or incorrectly processed transaction depends on the special conditions agreed for the respective order type (notably the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank).

11.2 Customer’s liability for misuse of the legitimation or security media

11.2.1 Liability of the Customer for unauthorised payment transactions prior to the suspension notice

The liability of the Customer is determined in accordance with the provisions of the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank, to which it is expressly referred to herein.

11.2.2 Liability of the Customer for other unauthorised transactions before a request to suspend access

The liability of the Customer is determined in accordance with the provisions of the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank, to which it is expressly referred to herein.

11.2.3 Liability of the Bank following the suspension notice

The liability of the Customer is determined in accordance with the provisions of the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank, to which it is expressly referred to herein.

11.3 Disclaimer

Liability claims are excluded in accordance with the provisions of the Specific Terms and Conditions for Payment Services of the Bank and the General Terms and Conditions of the Bank, to which it is expressly referred to herein.

12 Third-party banks; services from third-parties

(1) If accounts held at third-party banks are covered by the EDT Service, the Customer will in each case conclude separate agreements with these third-party banks about the type and scope of the EDT Service.

(2) If the Customer makes recourse to services from third-parties within the scope of the EDT Service, it shall be liable to the other party for all actions, errors or acts of omission by this third-party to the same extent as if it had performed the actions itself or were itself responsible for the acts of omission. For the purposes of these EDT Terms and Conditions, the third-party shall be deemed to be acting on behalf of the party that commissioned it.

(3) The Bank is not liable for any actions or omissions from third parties.

13 Effective Date and Application of the EDT Service

The EDT Terms and Conditions will apply as from the date of the acknowledgement by the Bank of the execution by the Customer or/and the Customer Affiliate of the EBICS Application Form and placing by the Client or/and the Customer Affiliate of the first order. Any new EDT Service activation, user`s creation, amendment, suspension, deletion, reactivation as well as the EDT Service cancellation is regulated by the EBICS Application Form.

The availability of the EDT Service for the Client of the Bank is subject to the maintaining of the business relationship with the Bank and will be cancelled upon termination of the business relationship with the Bank in accordance with its General Terms and Conditions.

14 Extension to Customer Affiliates; Appointment of Agent

(1) The extension of the EDT Terms and Conditions to any company belonging to the Customer's group of companies requires that the legal representative(s) of such a company acknowledges and executes the EBICS Application Form in accordance with the Clause 13 of the EDT Terms and Conditions.

(2) Upon acknowledgement and execution of the EBICS Application Form, such company becomes a "Customer Affiliate" under these EDT Terms and Conditions, and shall appoint the Customer as its agent to issue and receive all declarations and to perform all actions provided for in these EDT Terms and Conditions or considered by it to be necessary or useful in connection therewith. The Customer and the Customer Affiliate hereby warrant and represent to the Bank that, in connection with such appointment, the Customer and the Customer Affiliate have performed any acts, made any disclosures, and given any consents necessary to release the Customer from any restriction under any law against self-dealing or similar restrictions which would otherwise render its acting on behalf of a Customer Affiliate ineffective.

15 Governing Law; Submission to Jurisdiction

(1) The present EDT Terms and Conditions shall exclusively be governed by and construed in accordance with the Luxembourg law.

(2) Any litigation regarding these EDT Terms and Conditions shall be of the exclusive competence of the Courts of Luxembourg, Grand Duchy of Luxembourg, the jurisdiction of which the Customer agrees upon irrevocably, unless the Bank chooses to bring an action against the Customer before any other court having jurisdiction under ordinary rules of procedure, in particular according to the applicable jurisdiction rules of the relevant European regulations or applicable conventions.

16 General

The Annexes mentioned in these EDT Terms and Conditions form an integral part of the EDT Terms and Conditions and the EBICS Application Form as acknowledged and executed by the Customer or/and the Customer Affiliate- :

Annex 1a: EBICS Interface
Annex 1b: EBICS Specification
Annex 1c: Security requirements for the EBICS system
Annex 2: Specification of the data formats

Annex 1a: EBICS Interface

1 Identification and security procedures

The Customer (account holder) shall inform the Bank of the Subscribers and their authorisations with respect to the EDT Service.

The following identification and security procedures are used for EBICS:

- Electronic signatures
- Authentication signature
- Encryption

For each identification and security procedure the Subscriber has an individual key pair which consists of a private and a public key. The public subscriber keys shall be disclosed to the Bank in accordance with the procedures described in section 2 below. The public bank key must be protected against unauthorised alteration in accordance with the procedures described in section 2 below. The Subscriber's key may also be used for communication with other banks.

1.1 Electronic signatures

1.1.1 Electronic signatures of the Subscribers

The following signature classes are defined for the electronic signatures:

Individual signature (type "E")
First signature (type "A")
Second signature (type "B")
Transport signature (type "T")

"E", "A" and "B" type electronic signatures are referred to as qualified electronic signatures. Qualified electronic signatures are used for the authorisation of orders. Orders may require several qualified electronic signatures to be applied by different Users (account holders and their Attorney). For each supported order type, a minimum of number of qualified electronic signatures shall be agreed between the Bank and the Customer.

Type "T" electronic signature is designed to transport signatures and cannot be used to authorize orders, but only for transmission of orders to the bank system. "Technical Subscribers" (see section 2.2) can only be assigned a type "T" electronic signature.

The software used by the Customer can generate different messages (for example domestic and foreign payments orders, but also for messages concerning initialisation, reporting download and retrieval of account and transaction information, etc.) The Bank notifies the Customer of which message types can be used and which electronic signature type is to be used for this purpose.

1.2 Authentication signature

Unlike the electronic signature, which is used to authorize order data, the authentication signature only considers the control and login data of an individual EBICS message including the electronic signature contained therein. With the exception of a few system-related order types contained in the EBICS Specification, authentication signatures must be supplied by both the customer system and the bank system in every transaction step. The Customer must ensure that software is used which, in accordance with the EBICS Specification (see Annex 1b), verifies the authentication signature of each EBICS message transferred by the Bank while taking into account the current validity and authenticity of the Bank's saved public key.

1.3 Encryption

To ensure the security of banking data on the application level, the data is to be encrypted by the Customer in accordance and on the basis of the validity and authenticity of the stored public key belonging to the Bank according to the EBICS Specification (see Annex 1b).

In addition, transport encryption must be utilised for the external transmission path between the systems of the Customer and the Bank. The Customer must ensure the use of software that verifies, in accordance with the EBICS Specification (see Annex 1b) the current validity and authenticity of the server certificates applied by the Bank.

2 Initialisation of the EBICS interface

2.1 Registration of the communication interface

Communication is initialised by utilising a URL (Uniform Resource Locator). Alternatively, an IP address belonging to the Bank may be used. The Customer will be informed of the URL or IP on conclusion of the EDT Terms and Conditions.

To enable the EBICS interface, the Bank shall provide the Subscribers designated by the Customer with the following data:

- URL or IP address of the Bank
- Name of the Bank
- Host ID
- Permitted version(s) of the EBICS protocol and security process
- Partner ID (Customer ID)
- User ID
- System ID (for Technical Subscribers)
- Further specific details on Customer and Subscribers authorisations

For the Subscribers assigned to the Customer, the Bank will assign one User ID uniquely identifying it. In so far as one or more technical Subscribers are assigned to the Customer (multi-user system), the Bank will assign a System ID in addition to the User ID. If there are no Technical Subscribers defined, the System ID and User ID are identical.

2.2 Initialisation of the keys

2.2.1 First initialisation of the Subscriber keys

In addition to the general conditions described in section 1 above, the pairs of keys used by the Subscribers for the qualified electronic signature, the encryption of the order data and the authentication signature must also meet the following requirements:

1. The key pairs must be assigned exclusively and unambiguously to the Subscriber.

2. If the Subscriber generates the keys, the private keys must be generated by means which the Subscriber can keep under his / her sole control.

3. If the keys are made available by a third-party, it must be ensured that the Subscriber is the sole recipient of the private keys.

4. With respect to the private keys used for identification, each User shall define a password for each key which protects access to the respective private key.

5. With respect to the private keys used for protection of the data interchange, each User shall define a password for each key which protects access to the respective private key. It is possible to dispense with this password if the Subscriber’s security medium is stored in a technical environment protected against unauthorised access.

The Subscriber’s public key needs to be transmitted to the Bank for the Subscriber’s initialisation with the Bank. For this purpose the Subscriber shall transmit its public keys to the Bank via two independent communication channels:

- Via EBICS by means of the relevant system related order types,
- Via initialisation letter signed by the account holder or an authorised signatory.

For the Subscriber’s initialisation, the Bank shall verify the authenticity of the public subscriber keys transmitted via EBICS on the basis of the initialisation letter signed by the account holder or an authorised signatory.

The initialisation letter shall contain the following data for each public subscriber key:

- Purpose of the public subscriber key
- Electronic signature
- Authentication signature
- Encryption

- The respective version supported for each key pair
- Specification of the exponent length
- Hexadecimal form of the public key's exponent
- Specification of modulus length
- Hexadecimal form of the public key's modulus
  Hash value of the public key in hexadecimal form

The Bank will verify the signature of the account holder or Attorney on the initialisation letter and also whether the hash values of the Subscriber's public key transmitted via EBICS are identical to those transmitted in writing. If the verification is positive, the Bank will activate the relevant Subscriber for the agreed order types.

2.3 Initialisation of the Bank's keys

The Subscriber uses a specially provided system-specific order type to obtain the Bank's public key.

The hash value of the public bank key shall additionally be made available by the Bank via a second communication channel separately agreed with the Customer.

Prior to the first transmission via EBICS, the Subscriber shall verify the public bank keys sent by EDT by comparing their hash values with the hash values notified by the Bank via separately agreed communication channel.

The Customer shall ensure that software is used which verifies the validity of the server certificates used in connection with the transport encryption by means of the certification path that is separately provided by the Bank.

3 Placing orders with the Bank

The User shall verify the correctness of the order data and ensure that only the verified data are signed electronically. Upon initialisation of communication, the Bank first carries out subscriber-related authorisation verifications, such as order type authorisation or verification of possibly agreed limits. The results of additional banking verifications such as limit verifications or account authorisation verifications will later be notified to the Customer in the report. As an exception to this, the Customer may choose to agree to online verification of the order data by the Bank.

Orders transmitted to the Bank system may be authorised as follows:

1. All the necessary qualified electronic signatures are transmitted along with the order data.

2. If the use of distributed electronic signature ("verteilte elektronische Unterschrift – VEU") has been agreed with the Customer for the respective order type and the transmitted electronic signatures are insufficient for banking authorisation, the order is stored in the Bank system until all required electronic signatures are applied.

3. If the Customer and the Bank agree that orders transferred via EDT may be authorised by means of a single electronic signature, a transport signature (type "T") must be supplied for technical protection of the order data instead of the User's banking electronic signatures. To this end, this file must bear a special code (D-file) indicating that there are no further electronic signatures for this order other than the transport signature (type "T").

3.1 Placing orders by means of the distributed electronic signature (VEU)

The manner in which the distributed electronic signature will be used by the Customer shall be agreed with the Bank.

Distributed electronic signature shall be used where orders are to be authorised individually of the transport of the order data and, if applicable, by several Subscribers. Until all qualified electronic signatures necessary for authorisation have been applied, the order may be deleted by an authorised User. If the order has been fully authorised, only a recall pursuant to section 8 of the EDT Terms and Conditions can be made.

The Bank may delete orders that have not been fully authorised after expiry of the time limit separately indicated by the Bank.

3.2 Verification of identification by the Bank

An incoming order is executed by the Bank only after the necessary qualified electronic signature or the signed accompanying note has / have been received and positively verified.

3.3 Customer reports

The Bank will document the following transactions in the Customers reports:

- Transmission of order data to the banking system
- Transmission of information files from the banking system to the Customer's system
- Result of each verification of identification for orders from the Customer to the banking system
- Further processing of orders if they concern the verification of signatures and the display of order data
- Decompression errors

The Subscriber is obliged to inform itself on the result of the verifications carried out by the Bank by downloading the report promptly.

The Subscriber shall take this report, the contents of which correspond to the provisions of section 10 of Annex 1b, on file and submit it to the Bank upon request.

4 Change of the subscriber keys with automatic activation

If the validity period of the identification and security media used by the Subscriber is limited, the Subscriber must transmit the new public keys to the Bank in good time prior to the expiry date of such validity period. After the expiry date of the old keys, a new initialisation must be made.

If the Subscriber generates its key itself, the subscriber keys must be renewed using the order types provided by the system for this purpose on the date agreed to with the Bank. The keys must be transmitted in good time before expiration of the old keys. The following order types are to be used for an automatic activation of the new keys without renewed Subscriber's initialisation:

- Update of public banking key (PUB)
- Update of public authentication key and the public encryption key (HCA)

or, alternatively,

- Update of all three above mentioned keys (the public bank-technical subscriber key, the public identification and authentication key and the public encryption key) (HCS).

The PUB and HCA or HCS order types are to be assigned a valid qualified electronic signature. After the keys have been changed, only the new keys may be used.

If the electronic signature could not be positively verified, the process described in section 7 (3) of the EDT Terms and Conditions is followed.

The key may only be changed after all orders are complete processed. Otherwise, orders still unprocessed will have to be placed again using the new key.

5 Suspension of subscriber keys

If misuse of the subscriber keys is suspected, the Subscriber must suspend the access authorisation for all banking systems using the compromised key(s). If the Subscriber has the valid identification and security media, the Subscriber can suspend access authorisation via EBICS. If a message with order type "SPR" is sent, access will be blocked for the relevant Subscriber whose User ID was used to send the message. After suspension, the

Subscriber can place no further orders via EBICS until the access has been initialised again as described in section 2.

If the Subscriber is no longer in possession of valid identification and security media, the Subscriber can request suspension of the identification and security media outside the EDT process via the EBICS Application Form.

The Customer may request suspension of a Subscriber's identification and security media or of the entire EDT access via the EBICS Application Form.

Annex 1b: EBICS Specification

The specification is published on the website www.ebics.org.

Annex 1c: Security requirements for the EBICS system

In addition to the security measures described in Annex 1a item 5, the Customer must observe the following requirements:

- The software used by the Customer for the EBICS procedure shall comply with the requirements described in Annex 1a.
- EBICS customer systems may not be used without a firewall. A firewall is an application which supervises all incoming and outgoing messages and only allows known or authorised connections to pass through.
- The EBICS customer system must be configured in such a manner that the Subscriber has to login before the system can be used. The Customer must login as normal user and not as an administrator who is authorised, for instance, to carry out program installation.

Annex 2: Specification of the data formats

The specifications of the data formats are published on the website www.ebics.org.