CLEARSTREAM BANKING S.A.

and

Business Partner Framework Agreement

Table of Contents

This Business Partner Framework Agreement ("**Agreement**") is made and entered into between

CLEARSTREAM BANKING S.A., a *société anonyme* existing under Luxembourg law, having its registered office at 42 avenue J.F. Kennedy, L-1855 Luxembourg, registered with the Luxembourg Trade and Companies Register under the number B 9248

(hereinafter referred to as "Clearstream Banking")

And

(hereinafter referred to as the "**Business Partner**" or "**User**"),

Clearstream Banking and the User are individually referred to as a "**Party**", and collectively as "**Parties**".

PREAMBLE

WHEREAS, the Business Partner wishes to subscribe for certain services through the Xact Web Portal, which services will be separately subscribed for (the "**Services**").

WHEREAS, Clearstream Banking is willing to provide the Business Partner access to the Xact Web Portal to enable the provision of the Services to the Business Partner, upon the terms hereinafter provided.

WHEREAS, this Agreement provides a framework to subscribe to such Services.

NOW, THEREFORE, in consideration of the mutual agreements hereinafter set forth, it is hereby agreed between the Parties hereto as follows:

1. DEFINITIONS

1.1 The term "**Agreement**" shall mean this Business Partner Framework Agreement.

1.2 The term "**Certificate(s)**" shall mean a certificate that specifies the name of a Xact User and certifies that a public key, which is included in the certificate, belongs to that User. A digitally signed message is created with the aid of the private key that corresponds to the public key in this person's Certificate. A Certificate is issued and digitally signed by a certificate authority (CA). A Certificate's validity can be verified by checking the CA's digital signature, also called digital ID, digital passport, public-key certificate X.509 certificate and security certificate.

1.3 The term "**Clearstream Banking**" shall mean and refer to the duly licensed bank called Clearstream Banking S.A. organised as a *société anonyme* and incorporated under the laws of the Grand Duchy of Luxembourg.

1.4 The term "**Clearstream Banking's Source**" shall mean such third party licensors and owners of the Software and/or its components.

1.5 The term "**Documentation**" shall mean and refer to all documentation provided under the Agreement and any other documentation provided with the service to which the User has subscribed and to which this Agreement applies.

1.6 The term "**Smart Card(s)**" shall mean and refer to a secure cryptographic token used to perform cryptographic operations and to protect user credentials.

1.7 The term "**Software**" shall mean and refer to the computer software products specified in any Schedule, manuals, documentation or other materials supplied therewith.

1.8 The term "**Third Party**" shall mean any natural person or legal entity who is not a party to the Agreement; for the avoidance of doubt, subsidiaries and/or affiliates of the User are Third Parties.

1.9 The term "**Use**" of Software shall mean to load, utilise, store or display the Software.

1.10 The term "**Xact Services**" shall mean the Clearstream Banking connectivity services, to which the User has subscribed.

2. PURPOSE

2.1 Clearstream Banking is offering to the User the non-exclusive facility of using the Xact Web Portal and the Xact Services to enable the User to exchange information with Clearstream Banking and subscribe for the Services, in accordance with this Agreement.

2.2 By applying to the Xact Services and the Services, the User becomes a beneficiary of these services and shall not be considered as a customer in the primary sense within Clearstream Banking ICSD business activity.

2.3 Clearstream Banking shall provide the User with the Documentation, including without limitation technical specifications, user guides and security procedures. The User shall follow the requirements and procedures set forth in the Documentation, which may be revised from time to time.

3. CERTIFICATES AND SMART CARDS

3.1 For the purpose of using the selected Xact Services, the User will use a suite of security products (for example, passwords, Smart Card(s), Certificates, etc.).

3.2 The User shall exercise due care in safeguarding its Smart Card(s) or Certificates as well as in keeping confidential its PIN Code(s). Clearstream Banking shall not be responsible in the event of loss, theft, fraudulent or unauthorised use or for the performance of the User's Smart Card(s) and/or its PIN Code(s) or its Certificate(s).

4. SECURITY

4.1 The security Software is designed to the highest practical standards in terms of access, security, authentication and encryption.

4.2 The User agrees to be bound by and adhere to the security procedures set out in the Documentation, which Clearstream Banking may revise from time to time.

4.3 The User undertakes not to attempt to modify, circumvent or otherwise interfere with any of the security systems functions. Any such unauthorised activities will result in all warranties made by Clearstream Banking in relation to the security of the system being null and void.

4.4 The parties agree to comply with all the obligations set out in the Agreement on Information Security Requirements attached hereto as Annex [A].

4.5 The annexes to the Agreement shall be incorporated into and deemed part of the Agreement and all references to the Agreement shall include the annexes to this Agreement.

5. FEES

5.1 The Business Partner will pay the fee for the Services in accordance with the terms of the Fee Schedule agreed separately between the parties in relation to the relevant Service. Any taxes and fees due in relation to the conclusion or fulfilment of the Services, especially VAT, withholding tax, or any other tax shall be borne by the Business Partner at the prevailing rate and will be extra.

5.2 No power of attorney will be granted to any third party for invoice receiving or payment linked the Services provided to the Business Partner.

6. SUPPORT

Clearstream Banking shall provide appropriate product support on a best efforts basis and in accordance with the terms of the Xact Services to which the User has subscribed under the Agreement.

7. USERS LIABILITIES AND OBLIGATIONS

7.1 The Xact Services provided have been developed to operate in a technical configuration as specified on the Xact Web Portal User Manual. It is the responsibility of the User to ensure that the Xact Services operate in accordance with the operating system requirements and technical configuration described in the Documentation.

7.2 The User is responsible for the acquisition, installation, correct use, operation and maintenance of the technical configuration described in the Documentation.

7.3 The User is responsible for installing the Software mentioned in the system requirements (that is, Operating system, Browsers, Java) including upgrades and security patches to the Software according to the installation instructions described in the Documentation.

7.4 The User must take all reasonable security measures to ensure that access to the Xact Services is solely granted to persons properly authorised within its own entity. Clearstream Banking shall not be liable for the consequences of unauthorised access in any event.

8. CLEARSTREAM BANKING OBLIGATIONS

8.1 Clearstream Banking warrants for the sole benefit of the User that if properly installed and used in accordance with the Documentation the Xact Services provided comply with the specifications provided by Clearstream Banking in the Documentation.

8.2 Clearstream Banking undertakes to resolve, on a best efforts basis, any defects in the Xact Services identified by the User.

8.3 Clearstream Banking manages access to the Xact Services on a best efforts basis.

8.4 Clearstream Banking warrants to the User that it shall use commercially reasonable efforts to ensure that its IT infrastructure is free from any computer "virus" or any other malicious program code.

8.5 Components of the Xact Services are provided by third parties. Although Clearstream Banking has tested the third party components and warrants that such components meet the purpose for which Clearstream Banking has tested them, Clearstream Banking waives any responsibility for the availability and operation of third party software for any purpose for which the third party software has not been tested by Clearstream Banking.

8.6 In all other respects, Clearstream Banking shall only be liable if it acted with gross negligence or wilful misconduct.

9. TERM AND TERMINATION

9.1 This Agreement shall be valid for one (1) year from the date of execution. Beyond this initial term, the Agreement shall be renewed automatically and tacitly for successive periods of one (1) year unless terminated by Clearstream Banking or the Business Partner upon ninety (90) calendar days' written notice. Such notice can be served at any time.

9.2 In addition, Clearstream Banking reserves the right to terminate this Agreement and suspend the provision of any services provided under this Agreement with immediate effect, and without prior notice, if, in Clearstream Banking's opinion, the Business Partner is in material breach of any obligation incumbent upon it under the Agreement and/or the Documentation.

This also applies if circumstances arise that Clearstream Banking reasonably believes would materially affect the Business Partner's ability to fulfil the obligations incumbent upon it under the Agreement and/or the Documentation.

9.3 Notice of termination shall be in writing and shall be sent to the relevant party's correspondence address as notified to the other party in writing.

9.4 Upon termination of this Agreement for any reason, the Business Partner shall promptly return any and all Software, if applicable, and any associated materials and Confidential Information to Clearstream Banking and shall warrant in writing to Clearstream Banking that all copies or translations thereof have been returned to Clearstream Banking or destroyed.

10. CONFIDENTIALITY

10.1 The User undertakes to keep and treat as confidential and not to disclose to any third party any information of a confidential or proprietary nature concerning the Xact Services, their operability, Clearstream Banking's know-how, trade secrets, business transactions of which the User has been informed as a result of the execution of Agreement (the "**Confidential Information**") nor make use of such Confidential Information for any purpose whatsoever except for the purpose of carrying out its duties under the Agreement.

10.2 Information will not be considered Confidential Information if:

(a) already published or available to the public other than by a breach of the Agreement;

(b) rightfully received from a Third Party not in breach of any obligation of confidentiality;

(c) independently developed by personnel or agents of any party without access to the Confidential Information of the other.

10.3 The User shall take adequate safeguards to maintain the confidentiality of the Confidential Information by or to any other corporation, individual, firm or organisation, including, but not limited to, such specific safeguards as Clearstream Banking may request from time to time.

10.4 The User acknowledges that the Software and the Documentation, as well as all amendments, updates and new releases thereof supplied by Clearstream Banking and Clearstream Banking's Source contain proprietary, confidential and trade secret information developed or acquired by Clearstream Banking or Clearstream Banking's Source. The latter parties retain all trade secret rights thereto.

10.5 The receipt of any Confidential Information does not confer any intellectual property rights in the said Confidential Information to the User. Any technology, know-how, data or related product development, whether or not based, directly or indirectly, on Confidential Information ("**Clearstream Banking Know-How**") is and shall be the sole property of Clearstream Banking and all applicable rights in patents, copyrights, trademarks and trade secrets relating thereto

(the "**Property Rights**") shall remain the property of Clearstream Banking. The User undertakes not to sell, transfer, license, publish, disclose, display or otherwise make available the Clearstream Banking Know-How or the Property Rights without Clearstream Banking's prior written consent, to any third party, nor to use it for its own purposes or benefit except as provided herein.

10.6 The provisions of this Article 10 shall survive the expiration or termination of the Addendum.

11. DATA PROTECTION

11.1 Clearstream Banking is acting as independent data controller when performing its services and may have access to the personal data (within the meaning of the Clearstream Banking Notice of European Data Protection Terms) to the Customer with respect to the processing of the personal data.

11.2 Clearstream Banking undertakes to:

(a) Process the personal Data exclusively in accordance with (i) the terms of the GDPR Notice; (ii) the Contract, or (iii) the instructions received from the Customer from time to time, either orally or in writing; and

(b) Implement all appropriate technical and organisational measures necessary to ensure the safety and confidentiality of the personal Data against accidental or unlawful destruction or accidental loss, falsification, unauthorised dissemination or access and against all other unlawful forms of processing.

12. ASSIGNMENT

12.1 Neither Party may assign any of its rights or obligations under this Agreement without the prior written consent of the other Party. Subject to the preceding sentence, this Agreement will apply to, be binding in all respects upon and inure to the benefit of the successors and permitted assigns of the Parties.

13. WAIVER

13.1 The provisions of this Agreement may be waived, altered, amended or repealed in whole or in part only upon the written consent signed by duly authorised directors of the User and Clearstream Banking. The waiver by either Party of any breach of this Agreement shall not be deemed or construed as a waiver of any other breach, whether prior, subsequent or contemporaneous, of this Agreement.

13.2 No delay in exercising or enforcing, failure to exercise or enforce or partial or defective exercise or enforcement of any right, remedy, power or privilege given to either Party by or pursuant to this Agreement or by law and no custom or practice of either or both of the Parties at variance with the terms of this Agreement shall constitute or be construed as constituting a waiver or partial waiver by either of the Parties of any right, remedy, power or privilege, nor

shall it operate to prevent the exercise or enforcement of any right, remedy power or privilege at any subsequent time.

13.3 A Party seeking to waive any right, remedy, power or privilege shall give notice of waiver in writing signed by a duly authorised representative of that Party to the other Party.

14. MISCELLANEOUS

14.1 If any provision of the Agreement or the application of any such provision to any person or circumstance, shall be declared judicially or by arbitration to be invalid, unenforceable or void, such decision shall not have the effect of invalidating or voiding the remainder of the Agreement, and it is the intent and agreement of the Parties that the Agreement shall be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting therefore another provision that is legal and enforceable and that achieves the same objective.

14.2 In the event of conflict or inconsistency between any of the terms and conditions of this Agreement and any other terms or conditions printed or written upon any other document passing between the Parties, the provisions of this Agreement shall prevail. In the event of any conflict between the provisions of this Agreement and any of the Appendices, the provisions of this Agreement shall prevail.

14.3 Any headings contained in this Agreement are used only as a matter of convenience and reference and are in no way intended to define, limit, expand or describe the scope of this Agreement.

14.4 No advertising, publicity or similar public information nor any private communication to third parties concerning this Agreement shall be made by either Party without prior written consent of the other Party. Neither Party shall disclose any of the specific terms of this Agreement to any third party without the prior written consent of the other Party.

14.5 Nothing in this Agreement is intended to confer any benefit on any third party (whether referred to herein by name, class, description or otherwise) or any right to enforce a term contained in this Agreement.

14.6 This Agreement has been drafted in English language only, which language shall be controlling in all respects, and all other versions thereof in any other language shall be for accommodation only and shall not be binding upon the Parties. All communications to be made or given pursuant to this Agreement shall be in the English language.

14.7 Neither of the Parties will be bound by any terms, conditions, promises, decisions, definitions, warranties or representations with respect to the subject matter hereof other than as expressly provided herein, or as duly set forth on or subsequent to the date hereof in writing duly signed by the Parties hereto.

14.8 Clearstream Banking reserves the right to amend this Agreement. Clearstream Banking shall notify the Business Partner in writing by mail or by electronic means of any such amendment and of the effective date thereof. Unless the Business Partner shall inform Clearstream Banking in writing to the contrary within ten business days following the date of receipt of Clearstream Banking's notice, the Business Partner shall be deemed to have accepted such amendments.

15. NOTICES

15.1 Any notice or other communication to be given under or in connection with this Agreement or any agreement in connection with the Services shall be in writing and shall be sent to the address and facsimile number specified below (or to such other address or facsimile number as either Party may notify to the other pursuant to this provision). Any such notice may be delivered in person, by express courier, certified or registered mail, fax or other recognised method of electronic transmission, and shall be deemed given when received as evidenced by notice of confirmation of receipt, or (i) when sent by certified or registered mail, three (3) Business Days following deposit, (ii) when sent by express courier, two (2) Business Days following delivery to a commercially recognised international courier, charges prepaid, and addressed to the other Party at its then current or last-known address or, (iii) when sent via facsimile transmission with receipt of confirmation of successful transmission to the facsimile number provided.

To Clearstream Banking:	**To the User**:
Name: _____	Name: _____
Street: _____	Street: _____
Town: _____	Town: _____
Country: _____	Country: _____
email address: _____	email address: _____

15.2 To prove the giving of notice it shall be sufficient to prove that the notice was left or that the envelope containing such notice was properly addressed and posted by first class registered post or that the fax was transmitted.

15.3 Any change in address of either Party shall be promptly communicated in writing to the other Party.

15.4 Notwithstanding the foregoing, any payments made under this Agreement shall be deemed received only when actually received.

16. APPLICABLE LAW AND JURISDICTION

16.1 This Agreement shall be governed by and construed in accordance with the laws of Luxembourg.

16.2 The courts of Luxembourg-city shall have the sole and exclusive jurisdiction with respect to any Dispute between the Parties, arising out or in relation with this Agreement.

[remainder intentionally left in blank; signature page follows]

The Parties hereto, each by its duly authorised directors, have executed this Agreement in two (2) original copies as of the date written below. Each Party acknowledges having received one (1) original.

Clearstream Banking

_____

Name: _____

Title: _____

Date: _____

_____

Name: _____

Title: _____

Date: _____

The User

_____

Name: _____

Title: _____

Date: _____

_____

Name: _____

Title: _____

Date: _____

Annex A

Agreement on Information Security Requirements

PREAMBLE

The Business Partner (as defined in the Business Partner Framework Agreement) (the "**Partner**") and Clearstream Banking S.A., Avenue J.F. Kennedy 42, 1855 Luxembourg ("**CBL**") have entered into or intend to enter into a commercial relationship (the "**Cooperation**"). As result of such Cooperation, CBL will grant and the Partner will gain access to certain IT systems and components of CBL or its Affiliates (CBL and its Affiliates hereinafter also referred to as "**DBG**"). The provisions laid out in this document (the "**Agreement**") contain the Parties' agreement regarding the minimum IT security requirements, the Partner will comply with when accessing the IT systems of DBG.

§ 1. Definitions

For the purpose of this Agreement, the term

"Affiliate" means any person that, directly or indirectly, controls, is controlled by or is under common control with such Party; the term "control" means the possession of (i) 50% or more of the voting rights in the general meeting of a person or (ii) the power, directly or indirectly, whether by contract or ownership, to direct or cause the direction of the management and affairs of a person, including investment decisions;

"Confidential Information" has the meaning given to it in § 8 below;

"Cooperation" means the commercial relationship between the Partner and CBL;

"Disclosing Party" has the meaning given in § 8 below;

"Dispute" means any dispute, controversy, claim or difference of whatever nature arising out of, relating to, or having any connection with this Agreement (including a dispute regarding the existence, formation, validity, interpretation, performance or termination of this Agreement or the consequences of its nullity and also including any dispute relating to any non-contractual rights or obligations arising out of, relating to, or having any connection with this Agreement).

"Information Security" means the state of being protected from unauthorised modification, inspection, or other use of sensitive business information, as well as their, disruption, or destruction;

"Parties" refers to both the Partner and CBL;

"Party" refers to either Partner or CBL, as the case may be;

"Receiving Party" has the meaning given in § 8 below; and

"Representatives" means a Party's Affiliates as well as the directors, officers, employees, legal counsel, accountants, auditors, contractors and other representatives and advisors (including, without limitation, financial advisors, and consultants) of a Party or a Party's Affiliates.

§ 2. . General Information Security Requirements

1. The Partner shall appoint a member of its personnel to coordinate and manage information and technology security issues and processes related to the Cooperation. This employee shall act as primary contact person to DBG for any Information Security related matters.
2. The Partner warrants that its and client´s and its or its client´s customers' or members' IT-systems that are directly or indirectly interfacing with the IT-assets of CBL or any of its Affiliates use state of the art measures to protect such IT-systems against any viruses, worms, Trojan horses, rootkits, backdoors or other software, macros or information assets that could adversely affect any IT-assets or any services of CBL, its Affiliates or other CBL customers.
3. The Partner shall ensure that its IT systems and IT processes adequately and effectively ensure that the integrity, availability, authenticity, and confidentiality of DBG's data is not adversely affected by the Partner's access to DBG's IT-assets or services.

§ 3. Human Resources Requirements

1. The Partner shall ensure that its employees and contractors (i) are aware of Information Security threats and concerns, (ii) understand and fulfill their responsibilities in the context of Information Security, including the obligation to keep confidential information in confidence during and after their employment, and (iii) are suitable for the roles for which they were assigned to,
2. Partner shall perform appropriate background checks to verify the reliability of its personnel considering Information Security relevant aspects, based on the risk profile of the position, for example, by inspection of employee's police clearance certificates. All employment agreements for Partner's personnel shall be made in writing and include strict confidentiality obligations during and after the employment. Partner shall ensure, that its personnel is adequately trained regarding Information Security and security awareness.

§ 4. Access Control

1. The Partner shall have established and documented an access control policy on business and Information Security requirements that includes appropriate access control rules (logical and physical), access rights and restrictions for specific user roles towards their assets reflecting the associated Information Security risks.

2. The Partner shall

   • grant access to information, information processing facilities, network and network services only on a need-to-know and least privilege basis as required for the respective tasks and after proper authorisation;

   • ensure effective authentication and authorised user access (including privileged access), for example, by segregation of access control roles, access requests, access authorisations, access administrations;

   • determine a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services;

   • ensure that access rights of all employees and third parties to information and information processing facilities are removed or adequately adjusted upon change of role, responsibility, employment or contract as well as termination of employment, or contract that required access to the information or information processing facilities.

   • ensure that users access rights are reviewed and adequately adapted at regular intervals, which shall not be longer than six months for privileged user accounts and twelve months for all other user accounts;

   • prevent unauthorised access to information, application system functions, systems, networks, services and applications;

   • ensure that password management systems and password quality and complexity comply with generally accepted standards or the state of the art.

3. Regarding privileged access or access to information classified as major or critical, Partner shall

   • ensure that in addition access to information classified as major or critical is secured using two-factor authentication;

   • register and maintain all privileged access accounts in accordance with the information asset inventory;

- shall control activities of privileged user accounts and the use of network services handling information classified as major or critical, and shall, using a dedicated IT system, continuously monitor and log executed actions, user ID, time of information access and information modified. It is imperative that the protocols produced by the monitoring and logging system cannot be altered. Legitimate and prohibited behavior of privileged users shall be defined in applicable policies.

§ 5. Operations Security

1. The Partner shall implement and maintain rules and procedures for the installation of software on operational systems as well as operating procedures for all applications.

2. The Partner shall use effective measures including detection, prevention, and recovery controls, to protect its and DBGs infrastructure against malware. Partner personnel shall be adequately trained to be aware of the threats of malware and measures and methods to prevent and defend against such threats.

3. If the Partner operates its own systems or offers any form of software related service, the Partner shall have established a patch management process and patch their systems on a regular basis.

4. The Partner shall have established and implemented a backup policy which shall include requirements for the retention and protection of information. Backups shall be designed according to business requirements and risk levels relating to the unavailability of information.

5. The Partner shall have established and implemented processes for the recording, storing, and reviewing of event logs of user activities, exceptions, faults, and Information Security events. System administrator and system operator activities shall be logged, and the logs shall be protected and regularly reviewed.

6. The Partner shall have implemented and maintain processes for identifying and detecting vulnerabilities, especially on systems critical for the provisions of Partner's services or those processing or storing information classified as major or critical. The Partner shall continuously monitor and assess information about technical vulnerabilities of its information systems and take appropriate measures to address the associated risks. Any vulnerability is a weakness in security protection and must be dealt with effectively and efficiently when risk levels are unacceptable for the provisions of Partner's services or pose a risk to the Information Security of DBG. The Partner shall implement hardening measures and change configurations according to the identified risks.

§ 6. Communications Security

The Partner shall maintain and implement effective controls to ensure protection of information networks and its supporting IT assets, and to maintain the end-to-end security of information transferred within and outside of its organisation.

§ 7. Information Security Incident Management

1. The Partner shall have established and implemented management responsibilities and procedures for an effective and orderly response to Information Security incidents so he can respond accordingly.
2. The Partner notifies DBG promptly but in no case within more than 72 hours of any security incident in the information processing environment in relation to the Information handled and / or services provided by the Partner to DBG.

§ 8. Confidentiality

1. Confidential Information means all business, technical, proprietary, trade secret or other information disclosed or made available by DBG or its Representatives ("Disclosing Party") to the Partner or its Representatives ("Receiving Party") before or after the date of this Agreement, including without limitation information relating to the Disclosing Party's customers, products, services, operations, technologies, processes, methodologies, data, knowledge, know-how, software, algorithms, planned or existing computer systems and systems architecture, research and development, marketing plans and financial matters.

2. Confidential Information shall not include information that

   • at the time of disclosure by the Disclosing Party is publicly known;

   • following disclosure by the Disclosing Party becomes publicly known other than as a result of unauthorised disclosure by the Receiving Party or the Receiving Party's Representatives in breach of this Agreement;

   • prior to the time of disclosure by the Disclosing Party is known by or is in the possession of the Receiving Party or one or more of its Affiliates;

   • becomes available to the Receiving Party or one or more of its Affiliates from a third party which is not reasonably known by the Receiving Party or its respective Affiliate(s) to be prohibited by a contractual, legal, fiduciary or other obligation to the Disclosing

Party from disclosing the information to the Receiving Party or its respective Affiliates(s); or

• is lawfully and independently developed, discovered, or arrived at by the Receiving Party or any of its Representatives without use of Confidential Information

3. Other than with respect to the non-disclosure obligation of the third party in section 3 above, the Receiving Party shall bear the burden of proof for establishing one of the foregoing exceptions.

4. The Receiving Party shall keep the Confidential Information confidential and shall not disclose or reveal any Confidential Information to any third party without the prior written consent of the Disclosing Party. The Receiving Party may, however, disclose Confidential Information to its Representatives if they have a strict need to know such information for the performance of the contracts and the Receiving Party has procured compliance by its Representatives with confidentiality obligations protecting the Confidential Information, that are equivalent to the terms of this § 8. The Receiving Party agrees to be responsible for all use of Confidential Information by its Representatives and shall be liable for any breach of the confidentiality provisions caused, directly or indirectly, by its Representatives.

5. The Receiving Party and its Representatives may not use the Confidential Information for a purpose other than the performance of its obligations or the exercise of its rights under this Agreement and the Cooperation.

6. The Receiving Party shall use all reasonable efforts to keep the Confidential Information of the Disclosing Party in confidence and to safeguard the Confidential Information. In so doing, the Receiving Party shall take at least the same precautions which it would take to safeguard its own similarly valued proprietary and confidential information but shall in no event take less than commercially reasonable precautions. The Receiving Party shall take all measures (including court proceedings) to restrain or prevent any breach of the confidentiality obligations pursuant to this Agreement by its Representatives.

7. The Receiving Party shall not disclose to any third party any information that is protected by banking secrecy or stock exchange secrecy, whether such secrecy is established by law, by contract, or otherwise. The Receiving Party will impose on Receiving Party's personnel and on any commissioned sub-contractor an obligation to comply with banking secrecy and stock exchange secrecy. Upon DBGs request, the Partner will demonstrate its corresponding measures.

8. The Receiving Party or its Representatives may disclose Confidential Information to the extent:

• required by any applicable law or regulation (which shall, for the avoidance of doubt, include the requirement to inform the public of inside information under the European Market Abuse Regulation – MAR);

- requested by any binding order or directive of any court, governmental or regulatory authority having competent jurisdiction over the Receiving Party; or

- required pursuant to the rules and regulations of any stock exchange on which the securities of the Receiving Party or any of its Affiliates are listed;

provided, however, that the Receiving Party, unless prohibited by law (for example, by the requirement to inform the public of inside information under MAR), regulation or court or regulatory order to do so, (i) promptly notifies the Disclosing Party, orally or in writing, upon receipt of any request for disclosure of its Confidential Information; and (ii) reasonably cooperates with the Disclosing Party so as to provide the Disclosing Party with a reasonable opportunity, at its own expense, to (1) contest and assist in opposing any requirement of disclosure of its Confidential Information; (2) seek judicial protection against the disclosure; and (3) have such required disclosure be made under a protective order.

9. Upon receipt of a written request from the Disclosing Party at any time, the Receiving Party shall, and shall procure that its Representatives shall, promptly either (a) return to the Disclosing Party all documents or materials (including computer media) or such parts thereof containing or reflecting any Confidential Information in the possession or control of the Receiving Party or its Representatives or (b) permanently destroy, erase or delete all the Confidential Information in the possession or control of the Receiving Party or its Representatives, in particular, but not limited to, from any computer, mobile telecommunication device or similar device into which it was stored or programmed, and provide to the Disclosing Party written confirmation of such destruction, erasure or deletion.

10. The Receiving Party may, however, retain such Confidential Information which it is required to retain according to any applicable law or regulation, or which has been created pursuant to automatic archiving and back-up procedures. The General Legal Counsel of the Receiving Party may retain one complete set of Confidential Information solely for legal purposes. In all cases covered by this section any retained Confidential Information shall be retained on the terms of confidentiality set out in this Agreement, with the exception that it may be used as deemed necessary in litigation proceedings between the Parties or with third parties in connection with the Project and where such disclosure is necessary for the outcome of the proceedings.

11. Each Party acknowledges that neither the destruction or return, nor the deletion of any Confidential Information will release it from the obligations contained in this Agreement.

12. The Receiving Party acknowledges that the Confidential Information is of unique character and agrees that any direct or indirect breach of this Agreement will irreparably harm the Disclosing Party in a way that recovery of damages could not adequately compensate. Therefore, in the event of the Receiving Party's direct or indirect breach of confidentiality or non-disclosure, the Disclosing Party is entitled to the immediate termination of this Agreement and the Cooperation for cause and to an injunction or other equitable relief as may be deemed proper by a Court.

13. This Section and the confidentiality obligations hereunder shall survive the termination or expiration of the Agreement.

§ 9. Application of DBG Policies

Where the Partner's Representatives are granted direct access to DBG's infrastructure, either on site or via remote access (for example, via Citrix or similar solutions), the Parties agree that the Partner's Representatives shall follow the rules and limitations set out in the DBG Information Security Policy, Acceptable Use Policy, as well as the DBG Access Control and Infrastructure Policy, each in their respective most recent version at the time the Representative is being granted direct access. CBL will provide the Partner with the most recent version prior to the conclusion of this Agreement and will inform the Partner of any relevant updates without undue delay.

§ 10. Miscellaneous

1. **Waiver and variation.** A failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law, whether by conduct or otherwise, shall not constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement or by law, whether by conduct or otherwise, shall preclude or restrict the further exercise of that or any other right or remedy.

   A waiver of any right or remedy under this Agreement shall only be effective if given in writing and shall not be deemed a waiver of any subsequent breach or default.

   No variation or amendment of this Agreement shall be valid unless it is in writing and duly executed by or on behalf of the respective Party. Unless expressly agreed, no variation or amendment shall constitute a general waiver of any provision of this Agreement, nor shall it affect any rights or obligations under or pursuant to this Agreement which have already accrued up to the date of variation or amendment and the rights and obligations under or pursuant to this Agreement shall remain in full force and effect except and only to the extent that they are varied or amended.

2. **Force Majeure.** Neither Party shall be liable for failure or delay in performing any of its obligations under or pursuant to this Agreement if such failure or delay is due to any cause whatsoever outside its reasonable control, and it shall be entitled to a reasonable extension of the time for performing such obligations as a result of such cause.

3. **Severability.** Where any provision of this Agreement is or becomes illegal, invalid or unenforceable then such provision shall be deemed to be severed from this Agreement and, if possible, replaced with a lawful provision which, as closely as possible, gives effect to the intention of the Parties under this Agreement and, where permissible, that shall not affect or impair the legality, validity or enforceability in that, or any other, jurisdiction of any other provision of this Agreement.

4. **Governing law and jurisdiction.** This Agreement and any non-contractual rights or obligations arising out of or in connection with it shall be governed by and construed in accordance with the laws of Luxembourg. The parties irrevocably agree that the courts of Luxembourg shall have exclusive jurisdiction to settle any Disputes arising out of or in connection with this Agreement and waive any objection to proceedings before such courts on the grounds of venue or on the grounds that such proceedings have been brought in an inappropriate forum.

5. **Counterparts.** This Agreement may be executed in any number of counterparts. Each counterpart shall constitute an original of this Agreement but all the counterparts together shall constitute but one and the same instrument.