

DBRS FORM NRSRO

ANNUAL CERTIFICATION

EXHIBIT 3

March 2018

Exhibit 3

DBRS Annual Certification – March 2018

DBRS POLICIES AND PROCEDURES TO PREVENT THE MISUSE OF MATERIAL, NONPUBLIC INFORMATION

This Exhibit includes DBRS's confidential information policy statement and guiding principles, followed by a copy of its Confidential Information Global Policy.

Confidential Information Policy Statement

In the course of conducting its rating activities, DBRS may be exposed to confidential information regarding issuers and other parties. This information may include, among other things, contemplated business transactions or estimated financial projects. It may also include a credit rating action that has not yet been published on the DBRS website or through other readily accessible means.

DBRS analysts are required to exercise particular care when they confer with external parties, including subscribers to DBRS reports and representatives of entities rated by DBRS, to ensure that confidential information is not selectively or inadvertently disclosed.

DBRS has adopted the following four guiding principles upon which its policies and procedures to prevent the misuse of confidential information are based:

Confidential Information Guiding Principles:

Use Principle:

Confidential Information must only be used in the furtherance of DBRS's business, or as otherwise agreed with the client in a letter of engagement or confidentiality agreement. Use of Confidential Information for any other purpose, including for personal gain, is strictly prohibited.

Need-to-Know Principle:

A Covered Person must only share or pass along Confidential Information to another Covered Person that has the "need to know" the information to complete his or her job function(s). Confidential Information should only be stored where Covered Personnel who have a "need to know" can access it. If a Covered Person determines they have access to Confidential Information about which they do not have a "need to know", they must refrain from further accessing the Confidential Information and report the occurrence to their manager and notify Compliance, who will provide guidance with respect to further steps that may be taken.

Safekeeping Principle:

Covered Personnel must take reasonable steps to protect Confidential Information from fraud, theft and misuse, or inadvertent disclosure. DBRS expects Covered Personnel to adopt safekeeping practices consistent with those set out in the Employee Code of Conduct.

Release Principle:

DBRS generally does not disclose Confidential Information in response to outside requests.

SEE ALSO:

** Business Code of Conduct for the DBRS Group of Companies (See especially Sections 3.19 – 3.21)

dbrs.com/research/228896/internal/Code_Of_Conduct

** DBRS Rating Policies

dbrs.com/about/ratingProcesses

CONFIDENTIAL INFORMATION GLOBAL POLICY

Effective Date: December 1, 2017
Owner: Global Compliance
Applies to: All DBRS Covered Personnel

I. Purpose and Scope

This Confidential Information Global Policy ("Policy") sets out DBRS's approach to the identification and management of confidential information ("Confidential Information").

This Policy applies to all DBRS Covered Personnel in all jurisdictions and should be read in conjunction with the Insiders Procedure for Europe, the Personal Trading Global Policy and Global Procedure, and the Privileged Account Management Global Procedure. Capitalized terms are defined herein or in the Glossary.

II. Confidential Information

A. DBRS defines Confidential Information to include:

1. Data and information DBRS receives from or on behalf of an issuer or entity in connection with DBRS's business which DBRS knows, or should reasonably know, is information confidential to the issuer, entity or agent.

This does not include data or information that:

- i. was previously known to DBRS through independent sources;
 - ii. was lawfully received from a third party without an obligation of confidence;
 - iii. was in, or has become part of, the public domain;
 - iv. has been publicly released by the issuer, entity and/or its authorized agent on a prior basis;
or
 - v. is required to be released or disclosed by law.
2. Data and information with respect to a pending DBRS credit opinions that has not yet been publicly disclosed.
 3. Confidential Information further includes a class of price-sensitive information, known as Material, Non-Public Information ("MNPI").

B. DBRS defines MNPI as:

1. Information that has not been disclosed in such a way as to achieve a broad dissemination to the investing public generally, and:
 - i. if it were publicly known, that information would or would reasonably be expected to result in a significant change in the market price or value of a traded security; or
 - ii. there is a substantial likelihood that a reasonable investor would consider that information important in making an investment decision.

III. Confidential Information Framework – The Guiding Principles

Covered Personnel must not share Confidential Information except in accordance with this Policy and the following four guiding principles.

A. Use Principle

Confidential Information must only be used in the furtherance of DBRS's business, or as otherwise agreed with the client in a letter of engagement or confidentiality agreement. Use of Confidential Information for any other purpose, including for personal gain, is strictly prohibited.

B. Need-to-Know Principle

A Covered Person must only share or pass along Confidential Information to another Covered Person that has the "need to know" the information to complete his or her job function. In addition, Confidential Information must be stored where only Covered Personnel who have a "need to know" can access it. If a Covered Person determines they have access to Confidential Information about which they do not have a "need to know", they must refrain from further accessing the Confidential Information and report the occurrence to their manager and notify Compliance, who will provide guidance with respect to further steps that may be taken.

Although all Covered Personnel are subject to this Policy, any reduction in the number of individuals with access or knowledge of Confidential Information greatly reduces the likelihood that such information will be misused.

C. Safekeeping Principle

Covered Personnel must take reasonable steps to protect Confidential Information from fraud, theft and misuse, or inadvertent disclosure. DBRS expects Covered Personnel to adopt safekeeping practices consistent with those set out in the Employee Code of Conduct.

D. Release Principle

DBRS generally does not disclose Confidential Information in response to outside requests. Covered Personnel should report the request to their manager and notify Compliance, who will provide guidance with respect to further steps that may be taken.

IV. Prohibited Uses of Confidential Information

As noted above, Confidential Information must only be used in the furtherance of DBRS's business, or as otherwise agreed with the client in a letter of engagement or confidentiality agreement. Other uses of Confidential Information could result in disciplinary action or legal sanction.

In particular, Covered Personnel should note that each of the following may constitute a criminal and/or civil offence in some or all of the jurisdictions in which DBRS does business, and upon conviction, could result in the payment of fines and/or a prison sentence:

- acquiring or disposing of securities or investments, directly or indirectly, for your own account or on account of others, while in possession of related MNPI;
- recommending or inducing another person to engage in trading or dealing while in possession of



Insight beyond the rating.

related MNPI; and

- sharing MNPI with another person, other than in accordance with the Need To Know principle in section III.B herein or in the necessary course of business.

Any questions regarding the appropriate use of Confidential Information should be referred to the Chief Compliance Officer or the appropriate Regional Compliance Officer.

V. Permitted Sharing of Confidential Information

A. Sharing Confidential Information - The Need to Know Guiding Principle

Covered Personnel are only permitted to share Confidential Information, including MNPI, with other Covered Personnel when that other person needs to know the information to perform their job function.

B. Permitted Sharing within the DBRS Group of Companies

Confidential Information relating to credit opinions cannot be shared with anyone who is not within the DBRS entity (i.e. DBRS, Inc.) that is or will be issuing the rating, unless:

- the person is directly involved in the credit opinion, and
- has a “need to know” the information to perform their job function.

A person is “within the DBRS entity issuing the rating” if they are an employee, officer, or director of the DBRS entity this is issuing or will be issuing a credit opinion, or a consultant engaged by that entity.

While Independent Non-Executive Directors (“INEDS”) are “within the company” for which they serve as director, in accordance with separate procedures that DBRS employs with such directors, Confidential Information relating to a rating should **not** be shared with INEDs absent an exception granted by the Chief Compliance Officer.

C. Permitted Sharing With External Parties

Confidential Information relating to a credit opinion can only be shared with external parties if they are directly involved in credit opinion (e.g., the issuer or rated entity and their agents), or as otherwise permitted by the party that provided the Confidential Information.

A public rating that has not yet been published may only be shared with the Issuer and its agents.

D. Permitted Sharing with Regulators

Nothing in this Policy or otherwise limits an individual’s ability to communicate voluntarily and directly with an appropriate governmental entity or agency, including DBRS’s supervising regulators, concerning possible violations of law or regulation, or to provide information, including documents, not otherwise protected from disclosure by any applicable law or privilege, to such entities or agencies, or to cooperate with their investigative activities, and no individual is required to provide notice to or obtain consent from DBRS to do so. All provisions of this Policy should be construed in a manner consistent with the preceding sentence.



Insight beyond the rating.

VI. Tracking Access to MNPI

From time to time, regulators may ask DBRS for details regarding individuals within DBRS who received MNPI in connection with DBRS's business. In some cases, Covered Personnel may also be tasked to maintain a list of individuals with access to MNPI on an on-going basis. For more information regarding these circumstances, see the Insiders Procedure for Europe.

© 2017, DBRS Limited, DBRS, Inc., DBRS Ratings Limited and DBRS Ratings México, Institución Calificadora de Valores S.A. de C.V. (collectively DBRS). All rights reserved.