KYC Services Canada Privacy Policy

CONTENTS

1. Personal Data Protection Policy ("Policy")

The aim of this Policy is to set forth the rights and obligations in relation to Personal Data (as defined below) collected, processed and disclosed by or on behalf of IHS Markit KYC Services Limited ("**Provider**") in performing KYC Services for Subscribers with respect to Contributors with whom Subscribers' wish to do business (each, as defined below).

Provider maintains certain Personal Data about living individuals associated with Contributors, Subscribers and other third parties in both electronic and paper format, for the purposes of generating and supplying KYC entity profiles in accordance with the instructions of Contributors and Subscribers (the "**Services**").

Correct and lawful treatment of this Personal Data is paramount to maintaining confidence in Provider and for its successful operations.

This Policy should be read and understood by: (i) those associated with Contributors who provide Personal Data to Provider (so they may understand how Provider stores and uses this Personal Data), (ii) those associated with Subscribers who use the Services; and (iii) Personnel (as defined below) who access and handle Personal Data and (iv) any other person or entity with an interest in how Provider stores, handles, accesses or uses Personal Data.

The roles and responsibilities of Contributors, Subscribers and Provider in relation to the supply and use of Personal Data processed as part of the provision of the Services are described in greater detail in Appendix 1 of this Policy.

2. Definitions

"**Agreement**" means the agreement between Provider and the applicable Subscriber governing Provider's provision of the Services to the Subscriber.

"**Contributors**" are potential counterparties and clients of Subscribers;

"**Data Controllers**" are entities that determine the purposes for which and the manner in which Personal Data is processed;

"**Data Processors**" are entities that process Personal Data on behalf of, and in accordance with the instructions of, a Data Controller. Where Data Processors delegate some or all of such processing the delegate is referred to as a "**sub-processor**";

"**Canada Data Privacy Laws**" means all applicable laws and regulations relating to the processing of Personal Data and privacy in Canada, including (without limitation) where applicable the Personal Information Protection and Electronic Documents Act (PIPEDA), its regulations and any other applicable laws or regulations in force from time to time in Canada and its provinces protecting or regulating the collection, use, disclosure or retention of Personal Data, including

"**Data Subjects**" are living individuals residing in Canada who are the subject of Personal Data, including (without limitation) employees, agents and officers of Contributors and Subscribers;

"Governmental Authority" means any federal, national, supranational, state, provincial, local or other government, governmental, regulatory or administrative authority, agency or commission or any court, tribunal, or judicial or arbitral body.

"**KYC**" means Know Your Customer, which is a process used by Subscribers to verify the identity of Contributors who may become their clients;

"**Personnel**" are those individuals employed or contracted by Provider to provide the Services; and

"**Subscribers**" are clients of Provider who are identified as Subscribers in applicable agreements between Provider and its clients and include affiliates of, and authorised contractors for, parties identified as Subscribers in such agreements between Provider and its clients.

3. What Constitutes Personal Data?

Data is "**Personal Data**" if:

— It relates to an individual; and

— An individual can be identified from that data alone, or from that data when used in combination with information which Provider could access.

or if it otherwise falls within the scope of applicable Data Privacy laws.

Personal Data is "**Encryption Data**" if it includes Personal Data linked to or associated with any of the following (or is required to be encrypted under the Agreement or applicable Data Privacy Laws or is otherwise characterized by Provider as subject to encryption in connection with its processing):

— Social Insurance numbers;

— Federal or provincial health care or driver's license numbers;

— Financial account information;

— Medical, health or health insurance information;

— Military IDs;

— Passport information;

— Home addresses;

— Gender;

— Dates of birth;

— Resident or other types of Visas or work permits numbers; and

— Country of domicile or citizenship.

The types of Encryption Data that Provider will typically collect will include (without limitation) passport information, provincial health insurance numbers or driver's license numbers and military identification.

Specific obligations relating to the processing of Encryption Data by Provider are set out in Section 8 (Encryption Data Guidelines) of this Policy.

4. What Personal Data does Provider collect?

Provider collects various types of Personal Data (which will constitute, in some cases, Encryption Data) from Contributors and/or Subscribers. This Personal Data includes contact information and passport information from Contributors, Subscribers, or other third parties as well as the following types of information:

Data Attribute	Definition

Data Attribute	Definition
Role	The individual's role in the context of the entity's KYC profile (e.g., primary contact person, authorised signatory, compliance, credit, legal, closer, trader, admin agent).
Position	The individual's position/title at the entity for which he/she works.
First Name	The individual's first name.
Middle Name	The individual's middle name, if available.
Last Name	The individual's last name.
Directors - Individual: Last Name	The individual's last name.
Directors - Individual: Position/Role	The individual's position at the entity for which he/she works.
Directors - Individual: Title	The individual's designation (e.g., Mr., Ms., Mrs., Dr.).
Directors - Individual: Aliases (if applicable)	The individual's alias, if applicable.
Directors - Individual: Gender	The individual's gender if volunteered.
Directors - Individual: Date of Birth	The individual's date of birth
Directors - Individual: Residential address	The individual's address
Directors - Individual: Country of Citizenship	The individual's country of citizenship.
Beneficial Owner - Individual: Title	The individual's designation (e.g., Mr., Ms., Mrs., Dr.).
Beneficial Owner - Individual: First Name	The individual's first name.
Beneficial Owner - Individual: Middle Name	The individual's middle name, if available.
Beneficial Owner - Individual: Last Name	The individual's last name.
Beneficial Owner - Individual: Aliases (if applicable)	The individual's alias, if applicable.
Beneficial Owner - Individual: Gender	The individual's gender if volunteered.
Beneficial Owner - Individual: Address	The individual's address.
Beneficial Owner - Individual: Country of Domicile	The country where the individual resides.

Data Attribute	Definition
Beneficial Owner - Individual: Country of Citizenship	The individual's country of citizenship.
Beneficial Owner - Individual: Date of Birth	The individual's date of birth. Only applicable to Politically Exposed Persons (as defined in the Money Laundering Regulations 2007) or when additional due diligence requirements have been triggered.
Beneficial Owner - Individual: Government Issued ID Type	Type of identification as issued by a government for the individual. Government issued ID types must be current and must have a photo. Examples include passports, driver's licenses, military IDs, etc.
Beneficial Owner - Individual: Government Issued ID Number	Identification number as issued by the government for the individual. This number is captured in conjunction with the government ID type.
Related Parties - Individual: Title	The individual's designation (e.g., Mr., Ms., Mrs., Dr.).
Related Parties - Individual: First Name	The individual's first name.
Related Parties - Individual: Middle Name	The individual's middle name, if available.
Related Parties - Individual: Last Name	The individual's last name.
Related Parties - Individual: Aliases (if applicable)	The individual's alias, if applicable.
Related Parties - Individual: Gender	The individual's gender if volunteered.
Related Parties - Individual: Date of Birth	The individual's date of birth.
Related Parties - Individual: Country of Domicile	The country where the individual resides.
Related Parties - Individual: Country of Citizenship	The individual's country of citizenship.

Other similar information that helps confirm the identity of Contributors, or their officers, directors, representatives and employees may also be collected.

5. What use does Provider make of Personal Data?

Provider uses Personal Data for the purposes of generating KYC profiles on Contributors on the instructions of the Contributors or Subscribers and providing the Services to Subscribers with the permission of Contributors as more particularly described in **Appendix 1** (Performance) to this Policy.

In addition, Provider may use Personal Data it collects for operational, legal, personnel, regulatory, administrative and management purposes when instructed to do so by Contributors or where permitted or required to do so by

law. Examples of these uses may include providing products or services to Contributors or Subscribers, communicating with, or responding to requests by, Contributors, Subscribers or Data Subjects, responding to discovery requests, court orders, governmental or regulatory requests, or in connection with other legal, government or regulatory processes, complying with legal requirements and obligations to third parties, and asserting and defending claims in the context of litigation or other disputes.

6. To whom does Provider Disclose Personal Data?

Provider will disclose Personal Data to Subscribers, Provider affiliates, and/or sub-processors, contractors, and third parties engaged by Provider to the extent expressly permitted under the agreement with the Contributor and, in each case, exclusively in connection with providing Services to Subscribers on behalf of the Contributors.

In addition where Provider is holding Personal Data as a Data Processor it will do so pursuant to a written agreement with a Data Controller and will only disclose the Personal Data to third parties in accordance with the terms of the written agreement with the Data Controller unless expressly required to do so in order to comply with: (a) applicable court orders; or (b) requests from governmental or regulatory or quasi-governmental or regulatory authorities, organisations, bodies or agencies in respect of which the Data Controller has given its prior written consent and/or the Data Controller has been given sufficient opportunity to challenge any third party requirement for disclosure of the Personal Data and has not indicated an intention to make such a challenge.

To the extent practicable, Provider will aim to require any third parties that receive disclosure of Personal Data from Provider to confirm that they will comply with the relevant Data Privacy Laws and to treat Personal Data disclosed to them as confidential.`

Disclosure of Personal Data in the circumstances described above may involve transferring Personal Data to Provider's affiliates, sub-processors, contractors, or third parties engaged by Provider, or to Subscribers to locations both inside and outside of Canada and will only occur if Contributors and/or Subscribers have represented and warranted that (in respect of Personal Data of which they are Data Controllers) they have informed the Data Subjects ofsuch transfers in connection with the provision of the Service or if the transfer is otherwise permitted under Data Privacy Laws.

The extent to which Provider may make such transfers where it holds Personal Data as a Data Processor will be subject to the specific terms of the written agreement between Provider and the applicable Data Controller.

7. Processing of Personal Data

In addition to, and without limiting, Provider's obligations under the Agreement and any additional requirements mandated by the applicable Subscribers and/or Contributors, Provider will process such Personal Data in accordance with the terms set forth above, applicable Canada Data Privacy Laws and (without limitation) the principles set forth below:

— Include links to this Policy and the Online Privacy and Cookie Policy (as applicable) at http://www.kyc.com;

— Process Personal Data fairly and lawfully and in particular only use Personal Data for specified and lawful purposes;

— Only collect Personal Data that is adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

— Subject to its records retention policies, procedures and applicable law, not keep Personal Data for longer than is necessary for the purpose or purposes for which it is processed. Thereafter, Provider shall dispose of or de-identify Personal Data so it is anonymous and not identifiable of a Data Subject;

- Take appropriate technical and organisational measures against: (i) unauthorised or unlawful access, modification or processing of Personal Data, and (ii) accidental loss or destruction of, or damage to, Personal Data;

- Store Personal Data, on internal servers that are only accessible to persons who have a legitimate need to access such Personal Data; and

- When disclosing Personal Data to third parties, bind recipients to appropriate confidentiality, limited use, data protection and information security provisions.

8. Encryption Data Guidelines

In addition to, and without limiting, Provider's obligations under the Agreement and any additional requirements mandated by the applicable Subscribers and/or Contributors, Provider will process Encryption Data in accordance with the terms set forth above for Personal Data, applicable Data Privacy Laws and (without limitation) the following additional principles set forth below:

- Only process Encryption Data in accordance with these Encryption Data guidelines;

- Maintain a log and knowledge of the location of, and Personnel's access to, Encryption Data at all times;

- Encrypt all Encryption Data when transmitting on a public network (such as the internet), transmitting wirelessly or storing on a portable device such as a laptop, handheld device, thumb drive or disk or a machine that is connected to the Internet; and

- Upon disposal, shred Encryption Data (if in print) or degauss (if on electronic media).

9. Right to Access Personal Data

Under Canada Data Privacy Laws, Data Subjects have certain rights to review Personal Data relating to them and to require that the Personal Data relating to them be updated, corrected and deleted where is no longer needed for the purpose for which it was collected.

Any Data Subject wishing to exercise such rights should contact Provider's Information Compliance Officer at the address set out at the end of Section 11 of this Policy. Where a Data Subject contacts Provider, Provider shall determine whether the request relates to Personal Data it holds as a Data Controller or to Personal Data it holds as a Data Processor. Where the request relates to Personal Data it holds as a Data Processor, it shall forward the request to the Data Controller and notify the Data Subject as to the identity of the Data Controller to whom the request has been forwarded and Provider shall act in accordance with the instructions of the Data Controller unless applicable law provides otherwise. The right to review, update, correct and delete Personal Data may, subject to applicable Data Privacy Laws, be limited:

- If such requests are abusive or unreasonably excessive;

- Where the rights or safety of another person or persons would be prejudiced;

- By any applicable records retention policy or laws;

- If such request relates to existing or anticipated legal proceedings of which Provider, Contributors or Subscribers are aware; or

- If providing access would prejudice investigation of possible unlawful activity.

Provider shall take reasonable measures to verify the authority of the party making the request to access Personal Data before making it available and may charge an administrative fee in accordance with applicable Canada Data Privacy Laws.

10. Security Requirements

In accordance with, and without limiting, its obligations under its agreements with the Contributors and Subscribers, Provider will take appropriate technical and organisational security measures to maintain the confidentiality of Personal Data and to protect Personal Data against unauthorised or unlawful processing and accidental damage, loss or destruction. What is “appropriate” depends on the circumstances, taking into account (among other things) the complexity, nature and scope of Provider’s activities, the sensitivity of the information and the harm that may result from the security breach, which in itself may depend on the nature of the Personal Data.

11. Information Compliance Officer

Provider's Information Compliance Officer is responsible for ensuring the adequacy and implementation of this Policy within Provider.

Any questions or concerns about this Policy, or any concerns that Provider’s collection, storage, processing or disclosure of Personal Data is causing, or is likely to cause, substantial unwarranted damage or distress, should be addressed to the Provider Information Compliance Officer at the following email address: informationcompliance@kyc.com.

12. Exceptions to this Policy

Any requests for an exception to this Policy must be approved by the Provider’s Information Compliance Officer. Exceptions may be available to the requirements set out in this Policy on a case by case basis.

13. Updates to this Policy

Provider reserves the right periodically to review and, having complied with the Governance process and any other change control procedures set out in its agreements with Subscribers and/or Contributors as may be applicable in respect of any proposed changes, update this Policy as appropriate in connection with changes to the products or services offered by Provider, changes to the business operations of Provider, or changes to applicable laws. Any updates to this Policy shall take effect immediately upon confirmation unless otherwise stated.

APPENDIX 1: PERFORMANCE

In the context of the provision of the Services, different parties take different roles at different stages of the process. For clarity these are set out below.

1. **Collection, storage and disclosure of Personal Data by a Contributor for the purposes of generating completed entity KYC profiles for Subscribers:** In these circumstances, the Contributor determines the purposes for which, and the manner in which, the Personal Data it provides to Provider will be processed. These purposes are set out in the agreement between each Contributor and Provider and include generating KYC profiles for specific Subscribers authorised by the relevant Contributor from time to time. In these circumstances, Provider will only process Personal Data provided to Provider by the relevant Contributor on behalf of such Contributor and in accordance with the relevant Contributor's instructions from time to time (including those set out in the agreement between the Contributor and Provider (the **"Contributor Terms of Use"**)). The Contributor has represented and warranted in the Contributor Terms of Use that it has obtained all consents for the disclosure of Personal Data to Provider.

In some cases, Provider may delegate certain aspects of the processing of Contributors' Personal Data to certain related companies. In these circumstances, the related companies to which the processing is delegated would be considered to be sub-processors. These sub-processors may be situated outside Canada and the Contributor has represented and warranted in the Contributor Terms of Use that such delegation has been consented to by the relevant Data Subjects. Such sub-processors are engaged by Provider on terms and conditions that allow them to only process Contributors' Personal Data on Provider's behalf, in accordance with Contributors' instructions and the relevant Data Privacy Laws. The sub-processors will have entered into an agreement with the Provider containing substantially the same terms and conditions as are set out in the Contribution Terms of Use as it pertains to Personal Data protection.

In addition, Provider may verify certain of the Personal Data which has been disclosed to it by the Contributor or obtain Personal Data which the Contributor has not provided but which is necessary for the generation of KYC profiles (see next section for more detail) from publicly available sources such as company registration documents. In these circumstances, Provider processes such Personal Data on behalf of the Contributor because it has been instructed to do so pursuant to the Contributor's requirement that the KYC profile be prepared for disclosure to particular Subscribers.

2. **Provider discloses a KYC profile to a Subscriber:** In these circumstances the relevant Contributor to whom the KYC profile relates authorizes Provider to disclose the KYC profile to Subscriber.

3. **Receipt and Use of the KYC profile by the Subscriber:** The Contributor authorises Provider to release the KYC profile to the relevant Subscribers and these Subscribers receive the KYC profile and are free to use the KYC profile in the manner described in the Contributor Terms of Use.

4. **Subscribers provide Personal Data to Provider to allow Provider to provide them with KYC profiles:** The Personal Data provided by a Subscriber may include names and contact information of employees, agents or officers of the Subscriber and certain Contributors. In these circumstances, the Subscriber determines the purposes for which this Personal Data is processed (as set out in the relevant agreement between Provider and the Subscriber). Provider it will only process Personal Data in accordance with Subscriber's instructions and for no other purpose. The Subscriber has represented and warranted in the agreement entered into between Provider and the Subscriber that the Subscriber has obtained all consents for the disclosure of Personal Data to Provider.