KYC Services Australian Privacy Policy

Version 2.0/ 7th July 2017

CONTENTS

1. Australian Privacy Policy ("Policy")

The aim of this Policy is to provide guidance as to the rights and obligations in relation to Personal Data (as defined below) collected, held, used and disclosed by or on behalf of IHS Markit KYC Services Limited ("**Provider**") on behalf of Contributors and Subscribers (each, as defined below) in Australia.

Provider has a global Personal Data Protection Policy that applies in jurisdictions other than Australia. Provider's global Personal Data Protection Policy can be obtained by emailing informationcompliance@kyc.com.

Provider maintains certain Personal Data about Australian 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.

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 Privacy Laws**" means all applicable laws and regulations relating to the collection, storage, use and disclosure of Personal Data and privacy, including (without limitation) where applicable: (i) Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute to the Act, and the rules and regulations thereunder, all as may be amended or supplemented from time to time (ii) the European Union's Data Protection Directive (95/46/EC) or any implementing or related legislation of any member state in the European Economic Area including the Data Protection Act 1998 in the United Kingdom; (iii) the Japan Personal Information Protection Law; (iv) the Hong Kong Personal Data (Privacy) Ordinance; (v) the Privacy Act ; (vi) the Korea Real Name Financial Transaction Act; and (vii) any other applicable laws, regulations and guidance and codes of practice issued by any regulator established in a particular jurisdiction and all privacy and data protection legislation in any other applicable territory and any replacements, updates or supplements to any of the above.

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

"**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;

"Privacy Act" means the Privacy Act 1988 (Cth) as amended from time to time, including the Australian Privacy Principles; 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 is information or an opinion about an identified individual, or an individual who is reasonably identifiable:

— whether the information or opinion is true or not; and

whether the information or opinion is recorded in a material form or not, 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 collection, use, holding or disclosure of such information):

— Social Security numbers;

— Federal or state identification numbers or driver's license numbers;

— Financial account information;

— Medical, health or health insurance information;

— Military IDs;

— Passport information;

— Home addresses;

— Gender;

— Dates of birth;

— Alien registration numbers; and

— Country of domicile or citizenship.

The types of Encryption Data that Provider will typically collect will include (without limitation) passport information, utility bills, state identification or driver's license numbers and military identification (if applicable).

Some of the Encryption Data that Provider collects is "sensitive information" within the meaning of the Privacy Act. Sensitive information includes health information (such as any medical conditions an individual may have, details of any medical treatment an individual is receiving), racial or ethnic origin, sexual orientation or practices, religious or philosophical beliefs, criminal record, political opinions and membership of any political, professional or trade association or union.

Specific obligations relating to the Encryption Data collected, held, used and disclosed by Provider are set out in Section 8 (Encryption Data Guidelines) of this Policy.

4. What Personal Data does Provider collect?

Provider may collect various types of Personal Data (which will constitute, in some cases, Encryption Data) from Contributors and/or Subscribers. Ordinarily, Provider will not collect information directly from the Data Subject, as Provider will typically only deal with Contributors and Subscribers. Provider may also collect Personal Data about Data Subjects from third parties including from the employer of the Data Subject or from other relevant third parties, such as credit reporting bodies, law enforcement agencies and other government entities. In some cases, Provider may collect information directly from Data Subjects, such as where Data Subjects directly contact Provider. If Personal Data is not provided to Provider (whether by Contributors, Subscribers and other

third parties or directly by Data Subjects), then Provider may not be able to provide its services to Contributors and Subscribers and may not be able to answer any direct queries made by Data Subjects. Contributors and Subscribers may also decline to provide their own products and/or services to Data Subjects who do not provide their Personal Data for KYC purposes.

The Personal Data that Provider collects may include (without limitation) contact information and passport information from Contributors, Subscribers, or other third parties. The types of information that Provider will collect may include (without limitation):

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.

Data Attribute	Definition
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.
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.

Provider will not collect sensitive information about individuals unless it is strictly necessary for Provider to provide its KYC services or to manage its relationship with Contributors and Subscribers. Provider will ensure that the Contributor or Subscriber who has provided Data

Subjects' sensitive information to Provider has obtained the Data Subject's consent before collecting any sensitive information about a Data Subject and providing it to Provider.

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.

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, responding to complaints or investigations 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, related bodies corporate and affiliates of Provider, Provider's employees, 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.

To the extent practicable (or where required by applicable Data Privacy Laws), 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.`

7. Overseas disclosure of Personal Data

Provider may disclose personal information to its related bodies corporate and affiliates, some of which are located overseas, for some of the purposes listed above. Provider takes reasonable steps to ensure that the overseas recipients of Personal Data do not breach applicable privacy obligations imposed on Provider under Data Privacy Laws relating to the Personal Data of Data Subjects.

Provider may disclose Personal Data to entities located outside of Australia, including to:

— our Subscribers, who may be located in any country around the world, including countries in which Data Subjects' organisations or employers are located in or do business in;

— Provider's related bodies corporate and affiliates, located in the United States of America, the United Kingdom, India, Singapore and Hong Kong

— our data hosting and other IT service providers, located in the United States of America, the United Kingdom, India, Singapore and Hong Kong.

— other third parties located in the United States of America, the United Kingdom, India, Singapore and Hong Kong.

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 only use, hold and disclose 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 use, hold and disclose 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 and Correct Personal Data

Where Provider holds information that a Data Subject is entitled to access, Provider will endeavour to provide the Data Subject with suitable means of accessing it (for example, by mailing or emailing it to the Data Subject). Provider may charge Data Subjects a reasonable fee to cover its administrative and other reasonable costs in providing the information to Data Subjects. However, Provider will not charge for simply making the request and will not charge for making any corrections to Personal Data.

There may be instances where Provider cannot grant a Data Subject access to the Personal Data that it holds. Reasons for refusing access to a Data Subject's Personal Data include, amongst other things:

— when the giving of access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;

— when the giving of access would have an unreasonable impact on the privacy of other individuals;

— when the request for access is frivolous or vexatious;

— when the giving access would reveal evaluative information (such as any score card weighting system or score card result used by Provider) in connection with a commercially sensitive decision-making process; or

— when the giving of access would otherwise be unlawful or refusing access would be required or authorised under any Australian law or court or tribunal order.

If a Data Subject believes that the Personal Data that Provider holds about the Data Subject is incorrect, incomplete or inaccurate, then the Data Subject may request that Provider correct it. Provider will consider if the Personal Data requires correction. If Provider does not agree that the Data Subject's Personal Data is incorrect, incomplete or out of date, then Provider will add a note to the Personal Data stating that the Data Subject disagrees with it.

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 measures to protect Personal Data against from misuse and loss and from unauthorised access, modification or disclosure. What is "appropriate" depends on the circumstances, taking into account (among other things) the complexity, nature and scope of Provider's activities and the harm that may result from the security breach, which in itself may depend on the nature of the Personal Data.

Personal information is destroyed or de-identified when no longer needed or when we are no longer required by law to retain it (whichever is the later).

11. Complaints; Information Compliance Officer

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

If a Data Subject believes that their privacy has been breached, please contact the Information Compliance using the contact information below and provide details of the incident so that Provider can investigate it. Provider will treat complaints confidentially, investigate the complaint and aim to ensure that Provider contacts the Data Subject and that their complaint is resolved within a reasonable time (and in any event within the time required by the Privacy Act, if applicable).

Any questions or concerns about this Policy, or any concerns about Provider's collection, storage, use or disclosure of Personal Data 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 its 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 unless otherwise stated.

This Policy was last updated on 7th July 2017.