Data privacy notice

Effective Date: 25 May 2018

About SMBC Nikko Capital Markets Limited's use of personal data

SMBC Nikko Capital Markets Limited and its affiliate, SMBC Derivative Product Limited ("**we**", "**our**", "**us**" or "**SMBC Nikko**") respect an individual's privacy and comply with all applicable privacy laws in jurisdictions in which we provide our services. This Notice sets out how we, as data controller, will collect and use personal data.

In all cases, any complaints and requests to exercise data subject rights should be addressed to the Data Privacy Office at smbcnikkogdpr@smbcnikko-cm.com, 100 Liverpool Street, London, EC2M 2AT, United Kingdom.

In this Notice:

- "Data Protection Legislation" means all the applicable data privacy laws and guidance, including the EU General Data Protection Regulation (2016/679) ("**GDPR**") and, in the UK, the Data Protection Act 2018.
- "Personal data" means any information relating to an identified or identifiable natural person.
- "Special category data" means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

To whose personal data does this notice apply?

The Notice describes our practices when using personal data in the context of each client or supplier or agent to whom SMBC Nikko provides or receives any product or service and/or with whom SMBC Nikko enters into any transaction. This includes, for example, the personal data of the directors, officers, board members, staff members or shareholders of our corporate clients.

Personal data we collect

We collect certain personal data in the course of providing and receiving our services. We may collect the personal data directly from individuals through communications, applications or other forms, whether we receive these in writing or electronically. This information can include:

- Contact information we use to communicate with clients, suppliers and agents such as details of name, position, current and former addresses (private and professional), telephone number (private and professional), email address;
- Identity information we use to identify or authenticate individuals or to meet tax, anti-money laundering (AML) and other "Know Your Client" (KYC) legal and regulatory obligations, such as details of name, address (private and professional), employer, age/date of birth, nationality, sex, civil status, photograph, place of birth (City/Country), Individual Tax ID and information to assist us to determine whether the individual is a Politically Exposed Person (PEP), which may include information about criminal convictions if we are authorised to use this information under Data Protection Legislation). This may also extend to historic information about principals including past employment and qualifications.
- Financial information such as payments made and received and goods and services provided or purchased;
- Image capturing such as photographs taken at events, videos, and CCTV footage;

- Website information that is captured in our web logs such as device information, unique identification numbers (such as an IP address or device ID), browser information (e.g. URL, browser type, pages visited, date/time of access). This may also include information captured by our cookies, information captured regarding interactions with advertising information and behavioural information captured on users of the website.
- Communications information including communications by email, telephone or post in the course of communicating with clients, suppliers and agents and providing services to clients, including recordings of telephone calls; and
- Relationship information that helps us to understand more about how to conduct business with clients, suppliers and agents, their business requirements, and what types of products and services may interest clients.

Where we collect personal data from

This Notice applies when we collect individuals' personal data from third parties or when we collect it directly from the individual. We may collect personal data from third party sources, which include the following:

- Our corporate clients, suppliers and agents;
- Third party referrals;
- Checking and verification processes such as due diligence checks;
- Social media sites such as LinkedIn and other public internet sites;
- Insurance information bureaus and government or financial institutions; and

We may also collect personal data about individuals from our searches of third party sources such as the press, online publications, corporate registers, sanctions lists and databases of Politically Exposed Persons (PEP) for "Know Your Client" (KYC) and anti-money laundering (AML) purposes.

How and why we use personal data

We use the personal data we collect for the purposes of:

- Facilitating smooth running of the business through communication with corporate clients, suppliers and agents, for example, to communicate about the goods and services we receive from suppliers;
- Verifying identity, checking transactions for anti-money laundering (AML) purposes, assisting in the prevention of fraud, terrorist financing, bribery and corruption, tax evasion and assisting us to not provide services where individuals may be subject to economic or trade sanctions, on an ongoing basis, in accordance with our AML/KYC/PEP policies;
- Fulfilling a transaction initiated by us, such as the purchase of goods or services from suppliers;
- Fulfilling a transaction or providing a service initiated by a client;
- Sending communications by various methods, such as mail, email, fax, telephone and other channels;
- Maintaining and building upon client relationships and other business development activities;
- Maintaining business records of services, payments and other transactions; conducting audits for the legitimate purposes of the business, business planning and database management;
- Event management including inviting individuals to events;
- Internal product analysis and market research to help us develop and improve our services to clients and to better service their accounts;
- Maintenance of our systems, resolving issues and complaints internally as soon as possible to enable us to deliver high standards of service;
- Compliance with other contractual, legal and regulatory obligations;
- Fraud and theft prevention or investigation, or other security, crime prevention or risk management purposes; and

- Providing individuals on behalf of clients with more choices or information about products and services which may be of interest to our clients.

We justify our processing of personal data on the following legal bases:

- performing a legal obligation to which we are subject, which may include certain legal or regulatory requirements and recording services we provide by telephone;
- performing our obligations, or exercising our rights, under our contracts with clients, suppliers and agents;
- performing a task in the public interest, for example where we are carrying out our verification processes in relation to the prevention of fraud, money laundering, terrorist financing, bribery and corruption and to prevent the provision of financial and other services to persons who may be subject to economic or trade sanctions;
- pursuing our legitimate interests and those of third parties.

A legitimate interest will apply only where we consider that it is not outweighed by an individual's interests or rights which require protection of their personal data. We have determined that our legitimate interests include the following:

- Managing our business and our brand;
- The improvement and management of relationships with clients, suppliers and agents;
- Our compliance with our regulatory requirements and improving the overall performance of the business;
- The conduct of internal audits for the legitimate purposes of managing our business; • Investigating any complaints and providing client service;
- Obtaining professional (including legal) advice to protect our business and our brand;
- The sending of communications including marketing or other communications about products or services, where this is necessary to promote our services to clients;
- Taking steps to manage our credit, business and other risks as may be required to operate as an effective, efficient and financially prudent financial institution where this is necessary to pursue our legitimate interests in managing and protecting our business.

If an individual requires further information regarding our legitimate interests as applied to their personal data, they may contact the Data Privacy Office.

For limited purposes, such as in the case of certain marketing communications and undertaking anti-money laundering (AML), "Know Your Client" (KYC) and PEP (Politically Exposed Persons) checks and related actions, it may be necessary to process special category data. In these circumstances, we will process personal data only when there is a legal basis we can rely on under Data Protection Legislation. This may also include data about criminal convictions if we are authorised to use this information under Data Protection Legislation.

In certain circumstances, where an individual does not provide personal data which is required (for example, for us to carry out anti-money laundering (AML) checks), we will not be able to provide the products and services under our contract with clients or may not be able to comply with a legal obligation on us. We will make it clear if and when this situation arises and what the consequences of not providing the personal data will be.

Marketing communications

We will keep our clients up-to-date with details of our services by email / post using the personal data that individuals have supplied or which we have obtained about them. Individuals can opt out of receiving marketing as detailed below.

Additionally, we will ensure that any outside companies assisting us in marketing our products and services, or with whom we have marketing agreements, are under contractual obligations to protect the confidentiality of personal data, and to use it only to provide the services we have asked them to perform.

Who we share personal data about individuals with

We will disclose personal data of individuals as follows:

- To SMBC Nikko group companies for the purposes as set out in this Notice;
- To credit reference and other third party agencies and suppliers in order to carry out anti-money laundering (AML), "Know Your Client" (KYC) and Politically Exposed Persons (PEP) checks and comply with legal obligations;
- To third parties who have introduced clients, suppliers or agents to us, such as financial service providers in order to process the data for the purposes as set out in this Notice;
- To third parties who work on our behalf or for the clients to service or maintain client accounts, such as administrators and managers including those external to SMBC Nikko;
- To third parties who provide technical services to process transactions, such as suppliers of trading applications and other IT systems, and print services, which we use to process that personal data;
- To third parties who manage our physical premises;
- To third parties who service or maintain our business contact database and those who support our website;
- To third parties providing services to us such as our professional advisers (e.g. auditors and lawyers);
- To a party representing a client, supplier or agent (for example, in response to legal process);
- To competent authorities such as tax authorities, courts, regulators and other government agencies, security or police authorities where required or requested by law or where we consider it necessary (to the extent permitted by law);
- Subject to applicable law, in the event that SMBC Nikko is merged, sold, or in the event of a transfer of some or all of our assets (including in bankruptcy), or in the event of another corporate change, in connection with such transaction.

Where we will hold personal data

We may transfer and maintain the personal information of individuals covered by this Notice on servers or databases outside the European Economic Area (EEA), in particular to our group companies. In most cases, the specific country outside the EEA to which individuals' data may be sent is Japan.

Countries outside of the EEA may not have the equivalent level of data protection laws as in the United Kingdom. If we need to transfer personal data outside the EEA, we will take steps to make sure your personal data is protected and safeguarded once it leaves the EEA, in particular, the use of Model Clauses approved by the European Commission and permitted under Article 46 of the GDPR. If you would like to obtain the details of such safeguards, you can request these from the Data Privacy Office.

How long we will store personal data for

We will retain the personal data of individuals covered by this Notice for as long as required to perform the purposes for which the data was collected, depending on the legal basis on which that data was obtained and/or whether additional legal/regulatory obligations mandate that we retain the personal data. In general terms, this will mean that personal data will be kept for the duration of our relationship with the individual and:

- the period required by tax, company and financial services laws and regulations; and
- as long as it is necessary for individuals to be able to bring a claim against us and for us to be able to defend ourselves against any legal claims. This will generally be the length of the relationship plus the length of any applicable statutory limitation period under applicable law.

In certain circumstances, personal data may need to be retained for a longer period of time, for example, where we are in ongoing correspondence or there is a continuing claim or investigation.

What an individual's rights are in relation to the personal data

An individual will have certain rights in relation to their personal data. Some of these rights will only apply

in certain circumstances. If an individual would like to exercise, or discuss, any of these rights, they should submit their request in writing or email to the Data Privacy Office and provide sufficient information to allow us to understand the scope of the request.

- Consent: if our processing is based on consent, an individual can withdraw their consent at any time by contacting the Data Privacy Office.
- Access: an individual is entitled to ask us if we are processing their personal data and, if we are, they can request access to their personal data. This enables them to receive a copy of the personal data we hold about them and certain other information about it.
- Correction: an individual is entitled to request that any incomplete or inaccurate personal data we hold about them is corrected.
- Erasure: an individual is entitled to ask us to delete or remove personal data in certain circumstances. There are also certain exceptions where we may refuse a request for erasure, for example, where the personal data is required for compliance with law or in connection with claims.
- Restriction: an individual is entitled to ask us to suspend the processing of their personal data, for example if they want us to establish its accuracy or the reason for processing it.
- Transfer: an individual is entitled to request the transfer of their personal data to another third party in limited circumstances.
- Objection: where we are processing personal data based on legitimate interests (or those of a third party) an individual may challenge this. However we may be entitled to continue processing personal data based on our compelling legitimate interests or where this is relevant to legal claims. An individual also has the right to object where we are processing personal data for direct marketing purposes.
- Automated decisions: an individual is entitled to contest any automated decision made about them where this has a legal or similarly significant effect and ask for it to be reconsidered.
- Supervisory Authority: an individual also has a right to lodge a complaint with a supervisory authority, in particular in the Member State in the European Union where they are habitually resident, where they work or where an alleged infringement of Data Protection Legislation has taken place.

Changes to this Notice

From time to time, we may change and/or update this Notice. If this Notice changes in any way, we will post an updated version on our website.

If we change anything important about this policy (the personal data we collect, how we use it or why) we will highlight those changes at the top of the policy and provide a prominent link to it for a reasonable length of time prior to the change.

We recommend you regularly review this website to ensure that you are always aware of our data practices and any changes. Any changes to this Notice will go into effect on posting to this website.

How to Contact Us

If an individual wishes to exercise their individual rights, or to raise any questions, concerns or complaints concerning this Notice or our data practices, our Data Privacy Office can be contacted at: smbcnikkogdpr@smbcnikko-cm.com.