THIRD PARTY PRIVACY NOTICE
Scotiabank (Ireland) Designated Activity Company

Scotiabank (Ireland) Designated Activity Company ("**SIDAC**") is committed to respecting individuals' privacy.

SIDAC is incorporated in Ireland under number 30350 as a Designated Activity Company. SIDAC's place of business is the 5th Floor, IFSC House, IFSC, Dublin 1, Ireland.

For the purposes of data protection law, SIDAC is a data controller in respect of personal data that we process in connection with our business and the products and services that we provide. In this notice, references to "**we**", "**us**" or "**our**" are references to SIDAC.

1. About this privacy notice

As data controllers, we are responsible for ensuring that we use individuals' personal data in compliance with data protection law.

This privacy notice applies to the personal data we will gather in connection with the operation of our business and the products and services that we provide and sets out the basis on which we will process such personal data.

2. Personal data that we collect

We collect the following personal data about individuals:

- **Information that is provided by you directly or through your agent / company to us or one of our affiliates**. This includes information provided directly, whether by filling in forms, face-to-face, by phone, by letter, e-mail or otherwise. This information includes:

    - data collected whilst communicating with us, such as full name, gender, business or personal contact details (address, home and mobile telephone numbers), occupation, job position/title and area of responsibility, family details, marital status, location;
    - data gathered for due diligence purposes, for example, identification documents, including passport, date of birth, photographs, age, citizenship, nationality, residency, government issued identifying numbers (personal public service numbers/social security numbers), source of wealth/funds; and/or
    - other information, including in relation to credentials as part of recruitment and procurement activities, such as data provided on CVs and work history, regulatory registrations and work eligibility.

- **Information we collect or generate.** This includes information that we generate about staff at our customers or suppliers. This information includes:

    - interactions with our staff, captured in customer relationship management systems or in our email system (including but not limited to email address and the content, date and time of interactions and correspondence) or in communication devices or systems (including call recordings);
    - CCTV images and access records in respect of visitors to our office; and/or

- information provided on application forms.

- **Information we obtain from other sources**. This includes information that we obtain in connection with "know your customer" ("**KYC**") and anti-money laundering checks ("**AML**"), and information provided to us by an individual's employer in connection with our business relationship with the employer or for recruitment purposes. This information includes:

    - data collected via searches on publicly available sources, for example media/internet searches; and/or
    - data collected via a third party source (such as from an individual's employer, recruitment agencies or via our screening provider), including but not limited to, directorship searches, sanctions searches, criminal background checks and status as a politically exposed person or connection to politically exposed persons, and copies of identity documents.

3. Uses of personal data

Personal data will be stored and processed by us and/or our affiliates for the following purposes:

- to enable us to provide a range of products and services to our customers on an ongoing basis.

- for our legitimate interests, including:

    - to market our products and services to customers and potential customers appropriately;
    - to maintain our relationships with customers and for marketing or business development purposes;
    - to receive services from suppliers and manage and monitor our relationship with suppliers;
    - to effectively and efficiently administer and manage the operation of our business, for example in respect of business continuity arrangements, recruitment, investigating complaints and for risk management purposes;
    - to undertake audits, security and compliance monitoring, including of communications, to detect, investigate and resolve issues, cyber and other security threats, to monitor / test for compliance with policies, procedures and/or applicable law and regulation; and/or
    - to maintain our own books and records.

- to comply with legal and regulatory requirements, including record keeping, undertaking conflicts checks, reporting (including tax reporting) and responding to regulatory investigations and requests.

- to prevent and detect financial crime.

- to establish, exercise or defend our legal rights or for the purpose of legal proceedings.

4. Legal basis for using personal data

We will process personal data where there is a legal basis to do so. We are entitled to use personal data as outlined in this notice:

- to provide our products and services to our customers in accordance with our terms of business or other contracts with customers; if we are not provided with this information, we will not be able to carry out the relevant contract;

- where we have legal and regulatory obligations that we have to discharge;

- to establish, exercise or defend our legal rights or for the purpose of legal proceedings;

- in accordance with our legitimate interests (or the legitimate interests of one or more of our affiliates), as outlined in this notice under “Uses of personal data” above; and/or

- where applicable, in circumstances where individuals have consented or explicitly consented to the use of their data in a specific way.

5. Disclosure of personal data to third parties

Where applicable, we may disclose personal data to our affiliates for the purposes of:

- the management and administration of our business and our affiliates’ business; and/or

- ensuring and monitoring compliance with legal and regulatory obligations, for example trade and transaction reporting obligations, market abuse monitoring, KYC/AML monitoring and internal policies and procedures.

We take steps to ensure that personal data is accessed only by staff of such affiliates that have a need to do so for the purposes described in this notice.

We may share personal data with third parties (including service providers, professional advisors and contractors), enforcement/fraud prevention agencies, trading venues and regulators. Where applicable, this will include the following:

- information provided to service providers (for example IT and communications advisers, providers of our electronic data storage services), professional advisors (for example law firms, accountants and auditors) or contractors for the purposes of providing services to us;

- information provided to trading venues, enforcement/fraud prevention agencies and regulators to fulfil our legal and regulatory obligations and/or on a voluntary basis to our regulators, including in relation to investigations and financial crime reporting;

- in the event we sell any of our business or assets or are acquired, we will disclose personal data to the buyer if necessary, including for due diligence purposes; and/or

- information that we are required to disclose to the extent permitted by law, regulation or court order or to establish, exercise or defend our legal rights.

Third parties will be subject to appropriate data protection and confidentiality requirements under the terms of their contract with us. Trading venues and regulators will maintain their own privacy notices as controllers which can be viewed on the relevant websites.

6. Transfers of personal data outside the European Economic Area

We operate in Global Banking and Markets, which means that some of our affiliates and third party suppliers are located outside the European Economic Area (“**EEA**”). Therefore, the personal data that we collect may be transferred to, processed, and stored at, a destination outside the EEA.

Where we transfer personal data outside the EEA, we will only make such a transfer where an appropriate transfer mechanism is in place, in compliance with applicable data protection law. Where necessary, we will carry out a risk assessment to ensure that your personal data remains appropriately protected. This can be done in a number of ways, for instance:

- the country that we send the data to might be subject to European Commission adequacy regulations as offering a sufficient level of protection;

- the recipient might have entered into contractual commitments, in line with any legal requirements that apply, to make sure your personal data is adequately protected; or

- the recipient may be party to binding corporate rules (relevant to intra-group transfers only).

In other circumstances the law may permit us to transfer personal data outside the EEA by relying on an established derogation. The specific derogations that we are likely to rely upon for such transfers of personal data include:

- where a transfer may be necessary to establish, make or defend a legal claim;

- where the transfer is a one-off transfer which is necessary to meet our compelling legitimate interests;

- where the transfer is necessary for the performance of a contract (for example, where the transfer is in relation to a contract that has been entered into with you or is a contract that benefits you); or

- where the transfer is from a public register and meets the relevant legal requirements relating to access to that public register.

In all cases, however, we must ensure that any transfer of personal data is compliant with data protection law.

Individuals can obtain more details of the protection given to their personal data when it is transferred outside the EEA (including a copy of the standard data protection clauses) by contacting us in accordance with the "Contacting us" section below.

7. Retention of personal data

We will store personal data on necessary databases and personnel files, in soft and/or hard copy form. How long we hold personal data for will vary. The retention period will be determined by various criteria including:

- the purpose for which we are using it – we will need to keep the data for as long as is necessary for that purpose; and/or

- legal obligations – laws or regulation may set a minimum period for which we have to keep personal data.

Retention periods may be extended if we are required to preserve personal data in connection with legal proceedings. Upon request, we can provide more information on retention periods relating to your personal data.

8. Individuals' rights

Individuals have a number of legal rights in relation to the personal data that we hold. These rights include:

- the right to obtain information regarding the processing of personal data by us, and a copy of the personal data which we hold;

- where individuals have actively provided their consent for us to process personal data, the right to withdraw consent at any time. Please note that we may still be entitled to process personal data if we have another legitimate reason (other than consent) for doing so;

- the right to request that we rectify personal data if it is inaccurate or incomplete;

- the right to request that we erase personal data in certain circumstances. Please note that there may be circumstances where we may be asked to erase personal data but we are legally entitled to retain it;

- the right to object to, and the right to request that we restrict, our processing of personal data in certain circumstances. Please note that may be circumstances where we are legally entitled to continue processing personal data and / or to refuse such requests; and/or

- the right to lodge a complaint with the data protection regulator (details of which are provided below) if individuals think that any of their rights have been infringed by us.

Individuals can exercise their rights by using the details set out in the "Contacting us" section below and find out more information about these rights by contacting the Irish Data Protection Commission (https://www.dataprotection.ie).

9. Protection of personal data

We have implemented appropriate technical and organisational measures to protect personal data, which are required whether personal data is held electronically or in paper form and whether it is at rest or in transit. Technical measures, for example, include using encryption tools to protect personal data held in electronic form or pseudonymisation, where appropriate. Organisational measures, for example, include storing paper records containing personal data in locked cabinets and/or restricted areas.

10. Contacting us

Individuals who would like further information about the processing of their personal data, to make a related complaint or to exercise any of the rights listed above, should contact the Europe Privacy Department, c/o Compliance Department, Scotiabank (Ireland) DAC, IFSC House, IFSC, Dublin 1 or email: europedataprotection@scotiabank.com.

Where applicable, individuals may be required to supply a valid means of identification as a security precaution to assist us in preventing the unauthorised disclosure of personal data.

If you are unhappy with our processing of your personal data, you have the right to lodge a complaint with the Irish Data Protection Commission. Please visit https://www.dataprotection.ie for more information.

11. Changes

The content of this privacy notice may change from time to time and updated versions will be made available, including on our website (https://www.gbm.scotiabank.com/en/legal.html, under "Ireland Policies & Disclosures").