THIRD PARTY PRIVACY NOTICE

Scotiabank (Ireland) Designated Activity Company ("**SIDAC**") is a company incorporated under the laws of Ireland and registered with the Companies Registration Office in Ireland under number 30350. SIDAC's place of business is Three Park Place, Hatch Street Upper, Dublin 2, Ireland, DO2 FX65. SIDAC is committed to respecting individuals' privacy.

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

1. About this privacy notice

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 gather in respect of individuals (other than staff members) in connection with the operation of our business and the products and services that we may provide and sets out the basis on which we process such personal data. Please take the time to read and understand this privacy notice.

2. Types of personal data that we collect about you

We collect and process the following personal data about you:

- **Information that you provide to us directly, or through your agent / company or one of our affiliates**, for example by filling in forms, or communicating with us, whether face-to-face, by phone, e-mail or otherwise. Where applicable, this information includes:
  - recruitment information, such as data provided on CVs and work history;
  - business or personal contact details; and/or
  - data gathered for due diligence, verification, "know your customer" ("**KYC**") and anti-money laundering checks ("**AML**"), for example identification documents such as passports, and national insurance/social security numbers.

- **Information we collect or generate about you**, for example in relation to staff at our customers or suppliers and during recruitment. Where applicable, this information includes:
  - personal data related to recruitment, for example interview notes;
  - personal data that we collect through our communications with you, including video and call recordings, where applicable;
  - personal data that we collect through your attendance at our office, including CCTV footage/images, access records/pass and photographs; and/or
  - information in customer relationship management systems, such as business contact details and business meeting notes.

- **Information we obtain from other sources**. Where applicable, this information includes:

    - data collected for recruitment/onboarding purposes, for example in relation to interviews (including recordings, where applicable), regulatory registrations/status, fitness and propriety, screening and regulatory checks (including criminal offence data, where applicable), obtained via our screening service provider, and/or references from previous employers and recruitment agencies; and/or
    - in relation to our business, information for the purposes of due diligence, verification, KYC and AML processes, obtained via searches on publicly available sources, or your employer in connection with our business relationship with them or another third party source.

3. Uses of your personal data

Your 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, maintain customer relationships and undertake marketing and/or business development;
- to receive services from suppliers and manage and monitor our relationship with suppliers;
- to administer, manage and operate our business, including record keeping, recruitment, complying with contractual obligations and to ensure business continuity and resilience;
- to undertake audits, security, surveillance 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;
- to comply with legal and regulatory requirements, including record keeping and responding to regulatory investigations and requests;
- to prevent and detect financial crime; and/or
- to establish, exercise or defend our legal rights or for the purpose of legal proceedings.

4. Legal basis for using personal data

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

- where we have legal and regulatory obligations that we have to discharge;
- where it is necessary for our legitimate business interests, including:

    - to provide a range of products and services to our customers, maintain customer relationships and undertake marketing and business development;
    - to receive services from suppliers and manage and monitor our relationship with suppliers;
    - to effectively, efficiently and consistently administer, manage and operate our business;
    - to ensure business resilience/continuity and security, including physical, data/information and cyber;
    - to establish, exercise or defend our legal rights or for the purpose of legal proceedings; and/or
    - in the case of a sale or acquisition of our business activities.

- for criminal offence data, including allegations or investigations, to ensure compliance with regulatory requirements relating to unlawful acts and dishonesty, preventing or detecting unlawful acts, and to defend legal claims; and/or

- if applicable, where you have explicitly consented to the use of your data in a specific way, although please note that we do not generally rely on consent.

5. Disclosure of your information to third parties

We may disclose your personal data to our affiliates, including within any internal directories and databases, for the purposes of:

- providing a range of products and services to our customers, maintaining customer relationships and undertaking marketing and/or business development;

- the administration, management and operation of our business and our affiliates' business;

- complying with, and fulfilling, any functions that we and/or our affiliates may perform relating to, regional or global processes or management decisions; and/or

- ensuring and monitoring compliance with legal and regulatory obligations 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 your personal data with third parties including, where applicable, the following:

- information provided to service providers, including those performing outsourced or other services for us, such as pre-employment screening and background checks, or professional advisors for the purposes of providing services to us;

- information provided to enforcement/fraud prevention agencies and regulators to fulfil our legal and regulatory obligations, including in relation to transaction reporting, 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, for example 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 are subject to appropriate data protection and confidentiality requirements under the terms of their contract with us. Other data controllers, for example regulators, will maintain their own privacy notices which can be viewed on the relevant websites.

6. Transfers of personal data

Some of our affiliates and third party suppliers are located outside of 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.

We may transfer personal data to countries covered by European Union ("**EU**") adequacy regulations which have been assessed as offering an adequate level of protection to personal data, including, but not limited to, Canada, the United Kingdom and the EEA, and to US organisations self-certified under the EU-US Data Privacy Framework (also referred to as the EU-US data bridge).

Otherwise, where we transfer your personal data outside the EEA, we will only do so where an appropriate transfer mechanism is in place in compliance with applicable data protection law. For example, where the recipient has entered into a written contract to ensure your personal data is adequately protected, which is subject to the EU Standard Contractual Clauses and, where applicable, supplementary contractual measures.

Where necessary, we will carry out a risk assessment to ensure that your personal data remains appropriately protected.

In other circumstances, the law may permit us to transfer your 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); and/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 will ensure that any transfer of your personal data is compliant with data protection law.

You can obtain more details about the protection given to your 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

The period for which we retain your personal data is determined by various criteria, including:

- the purpose for which we are using your personal data – we will keep the data for as long as is necessary for that purpose.
- legal obligations – laws or regulations may set a minimum period for which we have to keep your 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. Your rights

Where applicable, you have a number of legal rights in relation to the personal data that we hold about you. These rights include:

- the right to obtain information regarding the processing of your personal data and access to the personal data which we hold about you;
- the right to withdraw consent regarding processing of your personal data. Please note that we do not generally rely on consent, but should we do so, we may still be entitled to process your personal data if we have another legitimate reason (other than consent) for doing so;
- the right to request that we rectify your personal data if it is inaccurate or incomplete;
- the right to request that we erase your personal data in certain circumstances. Please note that there may be circumstances where you ask us to erase your personal data but we are legally entitled to retain it; and/or
- the right to object to, and the right to request that we restrict, our processing of your personal data in certain circumstances. Please note that there may be circumstances where we are legally entitled to continue processing personal data and/or to refuse such requests.

You can find out more information about these rights by contacting the Data Protection Commission (https://www.dataprotection.ie).

9. Contacting us

If you would like further information about the processing of your personal data or to exercise any of the rights listed above, you should contact the Europe Privacy Department, c/o Compliance Department, Scotiabank (Ireland) DAC, Three Park Place, Hatch Street Upper, Dublin 2, Ireland DO2 FX65 or email: europeprivacy@scotiabank.com.

If you are unhappy with our processing of your personal data, please send your complaint to the Europe Privacy Department by email to europeprivacy@scotiabank.com. In accordance with our internal process, we will acknowledge receipt of your complaint and request additional information where required. Without undue delay, we shall:

- investigate and take appropriate steps to respond to your complaint;
- provide you with updates during the process, as appropriate; and
- confirm the outcome of your complaint to you.

In addition, you have the right to lodge a complaint with the Data Protection Commission. Please visit https://www.dataprotection.ie/ for more information and contact details.

Where applicable, you 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.

10. 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”).