

**HSBC Islamic Funds**  
*Société d'investissement à capital variable*  
16, Boulevard d'Avranches, L-1160 Luxembourg  
Grand Duchy of Luxembourg  
R.C.S. Luxembourg No. B 74 964

Luxembourg, 13<sup>th</sup> February 2020

**Privacy Notice**

**How we collect and use your personal information**

As an investor or potential investor in HSBC Islamic Funds (the "Fund"), we may collect and use personal data or information about you or individuals connected with you, including but not limited to your directors, employees and/or agents, representatives and/or beneficial owners and shareholders.

This notice explains how we will use that information, who we might share it with, and what steps we'll take to make sure it stays confidential and secure. This notice continues to apply even if your agreement with us (and/or your investment in the Fund) ends.

This notice applies to any personal data we receive from you (including any personal data that is provided in connection with your account such as information entered in the Fund's register of shareholders), create or obtain from other sources and explains how it will be used by us. If we've provided you with separate or further information about how we collect and use your personal information for a particular product or service, those terms will continue to apply to that service. If you interact with HSBC in a different context, e.g. as a banking customer or in a country outside the EU, separate terms will apply to that interaction.

It is important that you take the time to read and understand this notice so that you understand how we will use personal information relating to you, your directors, employees and/or agents, representatives and/or beneficial owners and shareholders and the applicable rights in relation to that personal information.

**Before we begin**

Wherever we've said 'you' or 'your', this means any individual who deals with us including individuals connected with you, such as but not limited to your directors, employees and/or agents, representatives and/or beneficial owners and shareholders. This notice only applies to information about individuals and not to information which is solely related to legal persons such as companies, trusts or pension funds.

Wherever we've said 'we' or 'our', this includes HSBC Investment Funds (Luxembourg) S.A. ("HIFL"), the Fund and other companies in the HSBC Group including the Fund's investment advisers, distributors and HSBC Bank plc., Luxembourg Branch acting as the Fund's depositary and central administrative agent. For the purposes of Regulation (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), HIFL and the Fund are the joint data controllers in relation to your information.

**What information we collect**

The information we collect or have about you might come from different sources. It may include information relating to any of our investment products or services (including any you may have applied for or held previously) or information we generate to improve our service and to manage, administer and take decisions about your account. Some of it will come directly from you in connection with your investment or potential investment in the Fund. Some of it might come from other HSBC companies. Some of it we might find from publicly available sources which we have lawfully accessed. Some of it might come from third parties or other organisations (e.g. fraud prevention agencies). Some information may be the result of combining different sets of information. We sometimes also record telephone conversations and monitor e-mail communications to resolve complaints or provide evidence of commercial transactions, improve our service and in order to comply with our legal and regulatory requirements.

This information may include:

- **Information that you provide to us.** This includes:
  - information about you that you give us when entering into an investment management agreement with us, applying for shares in the Fund by completing and returning the Fund's application form to us, or by communicating with us, whether face-to-face, by phone, e-mail, or otherwise. The information you give us may include your (and/or if applicable, your financial adviser or employee's) name, address, e-mail address and phone number, financial and tax status;
  - information concerning your identity to enable us to comply with anti-money laundering and counter-terrorism legislation (e.g. passport or identification information);
- **Information we collect or generate about you.** This includes:
  - client relationship information, payment and trade transactions information and other financial information;
  - geographic information;
  - information included in relevant documentation (e.g. record of advice) and other comparable information.
- **Information we obtain from other sources.** This includes:
  - communications information (e.g. email information, third party information, chat information, instant messages, corporate and media broadcasts, disputes / litigation, correspondence between solicitors and stakeholders and transcripts or minutes); and
  - combined information from external sources (e.g. information pertaining to interactions between individuals, organizations, prospects and other stakeholders acquired from companies that collect combined information and information from fraud avoidance systems).

*See expandable Appendix 1*

## **How we'll use your information**

We will collect information about you for various reasons as set out in this privacy notice, including to:

- manage and administer your accounts and holdings;
- carry out our services for the Fund;
- provide you with information, products and services you may request from us;
- verify your identity as part of our client onboarding process;
- detect and prevent fraud and money laundering in order to comply with applicable laws and regulations;
- identify politically exposed persons;
- carry out your instructions;
- improve our products and services;
- keep track of our conversations with you (by phone, in person, by email or any kind of communication including email screening);
- manage our relationship with you;
- corresponding with legal advisors, and third party intermediaries;
- manage our internal operational requirements for risk management, system or product development and planning, insurance, audit and administrative purposes.
- more generally in order to comply with all legal and regulatory obligations applicable to us (including compliance with tax reporting (i.e. FATCA, CRS) and anti-money laundering and counter-terrorism requirements)

Processing for any of the above purposes is necessary to enable us to pursue our legitimate business interests (or the legitimate interests of one or more of our affiliates). It may also be necessary for other reasons, as outlined below.

We will only use your information where we have a lawful basis for using it. These lawful bases include where:

- we need to pursue our legitimate business interests, such as enforcing the terms and conditions of any agreement we have with you;
- we need to process the information to perform our obligations under our contract with you;
- we need to process the information to comply with legal and regulatory obligations;
- we need to establish, exercise or defend our legal rights and / or for the purpose of (or in connection with) legal proceedings (including for the prevention of fraud); and,
- we have your consent, including consent for the use of cookies.

*See expandable Appendix 2*

Even if you ask us not to use your information, we may continue to use your personal information in circumstances where (a) the law says we have to; (b) we need to for the purposes of performing a contract; (c) we have a public interest to do so; or (d) we have a legitimate business reason for doing so.

### **Tracking or recording what you say or do**

We may record and keep track of conversations you have with us – including phone calls, face-to-face meetings, letters, emails, live chats, video chats and any other kinds of messaging in order to use these recordings to check your instructions to us and serve as evidence in court, assess, analyse and improve our service, train our people, manage risk, comply with our legal and regulatory obligations or to prevent and detect fraud and other crimes. We use closed circuit television (CCTV) in and around our offices for security purposes and so we may collect photos or videos of you, or record your voice through CCTV.

We may also perform email screening and related data controls to reduce the risks (for data integrity and confidentiality) relating to communication via email.

### **Who we might share your information with**

We may share your personal information with our affiliates or with entities external to the HSBC Group where:

- we need to in order to enforce or apply the terms of use and other agreements that you have with us;
- we need to for the purposes of providing you with investment products and services you have requested (e.g. pursuant to an investment management agreement);
- we have a public or legal duty to do so e.g. to assist with detecting fraud and tax evasion, financial crime prevention, regulatory and tax reporting, litigation or defending legal rights;
- we have a legitimate reason for doing so e.g. to manage risk, verify your identity, or assess your suitability for products and services;
- we have asked you for your permission to share it, and you've agreed;
- we need to ensure the safety and security of our data; or
- we need to for internal research and statistical analysis purposes.

We may transfer and disclose your information to:

- other HSBC group companies and any sub-contractors, agents or service providers who work for, or provide services to, us or other HSBC group companies (including their employees, sub-contractors, directors and officers);
- anyone who deals with us in relation to your investment and agreement with us (e.g. financial adviser), the people you make payments to, your beneficiaries, intermediary, correspondent and agent banks, clearing houses, clearing or settlement systems, market counterparties, upstream withholding agents, swap or trade repositories, stock exchanges, and any companies you hold securities in through us (e.g. stocks, bonds or options);
- other financial institutions, fraud prevention agencies, tax and supervisory authorities, trade associations, credit reference agencies and debt recovery agents;
- any person, company or other entity that has an interest in or takes on the risk in relation to or in connection with the products or services that we provide to you;

- any prospective or new HSBC companies (e.g. if we restructure, or acquire or merge with other companies) – or any businesses that buy part or all of any HSBC company;
- to auditors, regulators or dispute resolution bodies and to comply with their requests;
- if there's a dispute over a transaction, anyone else who's involved;
- law enforcement, government, courts, or our regulators; or
- fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity.

### **Sharing Aggregated or Anonymised Information**

We may share aggregated or anonymised information outside of HSBC with partners such as industry associations. For example, we may share such information publicly to show trends about the general use of our services. However, you won't be able to be individually identified from this information.

### **How long we'll keep your information**

How long we hold your personal information 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
- legal obligations – laws or regulation may set a minimum period for which we have to store your personal data.

### **Transferring your information overseas**

Your information may be transferred to, and stored at, a destination in the European Economic Area (“**EEA**”), such as the United Kingdom, France, Italy, Spain, Belgium, Germany and outside the EEA (i.e. Switzerland), including to locations which may not have the same level of protection for personal information such as, but not limited to, Malaysia, Sri Lanka and Hong Kong. We may need to transfer your information in this way to perform our contract with you, to fulfil a legal obligation, to protect the public interest and/or for our legitimate business interests.

Where we transfer your information outside the EEA (including in countries which are not subject to an adequacy decision of the European Commission or which do not ensure an adequate level of protection of personal data), we will ensure that it is protected by us in a manner that is consistent with how your information will be protected by us in the EEA. We will always do this in a way that is permissible under data protection law.

You can obtain more details of the protection given to your information when it is transferred outside the EEA by contacting us in accordance with the “More details about your information” section below.

### **Your rights**

You have a number of rights in relation to the information that we hold about you. These rights include:

- the right to obtain information regarding the processing of your information and access to the information which we hold about you;
- in certain circumstances, the right to withdraw your consent to our processing of your information at any time, without prejudice to the lawfulness of the data processing carried out before the withdrawal of such consent. Please note, however, that we may still be entitled to process your information for other purposes than the ones covered by and for which we obtained your consent if we have another legitimate reason for doing so;
- in some circumstances, the right to receive some information electronically and/or request that we transmit the information to a third party where this is technically feasible. Please note that this right only applies to information which you have provided to us;

- the right to request that we rectify your information if it is inaccurate or incomplete;
- the right to request that we erase your information in certain circumstances. Please note that there may be circumstances where you ask us to erase your information but we are legally entitled to retain it;
- the right to object to and the right to request that we restrict our processing of your information in certain circumstances. Again, there may be circumstances where you object to, or ask us to restrict, our processing of your information but we are legally entitled to continue processing your information and / or to refuse that request; and
- the right to lodge a complaint with the data protection regulator (in Luxembourg, the *Commission Nationale pour la Protection des Données*: <https://cnpd.public.lu/en.html>) if you think that any of your rights have been infringed by us.

You can exercise your rights by contacting us using the details set out in the “More details about your information” section below.

### **What we expect from you**

You are responsible for making sure the information you give us is accurate and up-to-date. And you must tell us if anything changes, as soon as possible. If we ask you for any information and you do not provide it to us, we may need to stop providing products and services to you and refuse to accept investments in the Fund.

**If you give us any personal information that does not relate to you (e.g. information about your financial adviser and/or your employees or representatives and/or beneficial owners and shareholders of companies, trusts, pension funds or other legal entities that may be entered in the Fund’s shareholder register) including any personal data that is provided in connection with your account such as information entered in the Fund’s register of shareholders, you must tell the relevant persons in writing what information you have given to us and how we process it (as set out in this notice) and, if applicable, obtain the necessary consent to process such personal information. You must also tell them how they can exercise the rights set out in this notice, such as for example how they can see what information we have about them and correct any mistakes.**

Some of the links on our websites lead to other HSBC or non-HSBC websites, with their own privacy and information protection policies, which may be different to this notice.

### **How we keep your information secure**

We implement internal technical and organisational measures to keep your information safe and secure which may include encryption, anonymisation and physical security measures. We require our staff and any third parties who carry out any work on our behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of information.

### **More details about your information**

If you would like further information on any of the information above, please address questions, comments and requests to HSBC Investment Funds (Luxembourg) S.A. at [hifl.gdpr.queries@hsbc.com](mailto:hifl.gdpr.queries@hsbc.com)

This Privacy Notice may be updated from time to time, please see the latest version here:

<http://www.global.assetmanagement.hsbc.com/Luxembourg/privacy-notice>

## Appendix 1 – Information we collect about you

- **Contact details** such as your name, date and place of birth, and nationality, postal address, telephone number, email address;
- **Identification information** such as passport ID, date of birth, picture, paper copy of identity;
- **Payment Transactions Data:** such as records from our payments processing systems that contain the information about executed transactions and includes order information (e.g. payment order), payment information and other information from the fulfilment of our contractual obligations (e.g. sales information in payments processing);
- **Other Financial Data:** including information regarding your financial situation (e.g. information regarding your tax status or the source of your assets);
- **Risk Data / Ratings:** risk identification information (incl. country domiciliation), transactional behaviour, client due diligence and periodic review results, financial crime risk management (FCRM) rating (high/medium/low), external intelligence reports, screening alerts (e.g. Transaction Screening, Name Screening, AML), unusual activity information (to develop (SARs) / and UARs).
- **Investigations Data** (Information pertaining to results from investigations on internal HSBC business practices, processes and operations). Grey information (e.g. allegations of wrongdoing, considered unproven, highly sensitive, may be structured or unstructured.)
- Data pertaining to known or suspected risk associated with clients, acquired from external watchlists and internal risk intelligence systems (e.g. Risk / Case Management).
- Data and artefacts required to support compliance to regulations that require screening of clients, their transactions and detection of suspicious and unusual activity.
- **Profile Data for KYC purposes** such as Individual identity and reference information, information published on the internet or which has been received from external providers; publically available or internally collected identity and demographic reference information about individuals who may be HSBC customers, connected parties, prospects, stakeholders or not at all related with HSBC (e.g., marketing lists) that contain personally identifiable information.
- **Information Security Risk Data;** External information used to manage the information security threat environment, including watchlists, lists of bad URLs and known bad IP addresses, threat and vulnerability alerts, and information breach intelligence reports and news. Known actors (cyber criminals), external email addresses, leaked information lists (e.g. external breaches which has employees involved), acquired credit card / account details;
- **Communications Data:** e.g. email information, third party information, chat information, instant messages, corporate and media broadcasts, disputes / litigation, correspondence between solicitors and stakeholders and transcripts or minutes.
- Information pertaining to results from investigations on internal HSBC business practices, processes and operations. Content and meta-data related to exchanges of information between and among individuals, organizations, workers, prospects, customers, other stakeholders and HSBC. Electronically recorded communications in the form of voice, email, or chat; corporate media communications, operational communications between two or more individuals or organizations regarding any HSBC activity that is directly or indirectly supporting customer servicing, third-party relationship and fulfilment.
- **Complaints information;** including disputes / litigation (legal case and matter information including legal strategy, document production, deposition and court transcripts, legal billing and time booking information).
- **Cookie Information:** IP Address, Browser behaviour etc.
- **Unusual Activity Reports (UAR) and Suspicious Activity reports (SARs).**

## Appendix 2 – How we use the information

We will use your information for the following purposes:

- 1. Deliver our products and services, or process your transaction in order to meet your investment objectives:** We will use your information to provide you with our products and services and to process your transactions. We will do this in line with our legitimate interests, legal obligations and in order to perform our contract with you.
- 2. Compliance with Laws and Regulations:** comply with the law, or any relevant rules or regulations. This may include to help detect or prevent crime (including terrorism, money laundering and other financial crimes), filing of relevant reports to regulators and/or authorities (including tax reportings, FATCA, CRS...), disclosing information to authorities, regulators or government agencies to fulfil our legal obligations. This is carried out to comply with legal obligations, because it is in the public interest, and because it is in our legitimate interest to do.
- 3. Preventing and Detecting Crime:** We will use your information to take measures to prevent crime including fraud monitoring and mitigation and fraud risk management, carrying out customer due diligence, name screening, transaction screening and customer risk identification, in order to comply with our legal obligations, because this is in the public interest to carry out and assess risk in our legitimate interest. We may share your information with fraud agencies, law enforcement and other third parties where the law allows us to for the purpose of preventing or detecting crime. Additionally we may take steps along with other financial institutions to help prevent financial crime and manage risk where we have a legitimate business interest or public interest to do so, such as where it is important to prevent or detect crime. We may be required to use your information to do this, even if you have asked us to stop using your information. That could include (among other things):
  - screening, intercepting and investigating any payments, instructions or communications you send or receive (including drawdown requests and application forms);
  - investigating who you're paying or who's paying you e.g. checks on payments in and out of your account;
  - passing information to fraud prevention agencies, if we think you've given us false or inaccurate information, or we suspect fraud;
  - combining the information we have about you with information from other HSBC companies;
  - checking whether the people or organisations you're paying or receiving payments from are who they say they are, and aren't subject to any sanctions.
- 4. Security and Business Continuity:** we take measures to aid business continuity, information security and we undertake physical security activities in order to fulfil our legal obligation and for internal risk strategy purposes as required in our legitimate interest.
- 5. Risk Management:** We will use your information to measure, detect and prevent the likelihood of financial, reputational, legal, compliance or customer loss. This includes credit risk, traded risk, operational risk & insurance risk. We will do this to fulfil our legal obligation and also because we have a legitimate interest in using your information for these purposes.
- 6. Product & Service Improvement:** We will use your information to identify possible service and product improvements (including profitability) by analysing information. The lawful basis for processing your information for this purpose is our legitimate interests.
- 7. Cookies:** When using any web-based applications, we will ask for your consent to our use of cookies. The lawful basis for processing your information for this purpose is consent.
- 8. Information as a product:** Where we collect your information for another purpose, e.g. for client on boarding, we may share such information or analytics results with third parties including other HSBC entities where it is in our legitimate interest to do so. The information may be presented as research whitepapers, the delivery of customer-specific information or insights back to same customer, credit checks, and anonymisation of information for the wider market. If we need to process your information for any other purpose, we will notify you with details of the new purpose (and obtain consent, if required) prior to that further processing.

9. **Protecting our legal rights:** We may need to use your information to protect our legal rights such as in the case of defending or the protection of legal rights and interests (e.g. collecting money owed; defending rights of intellectual property); court action; managing complaints or disputes; in the event of a restructuring of companies or other mergers or acquisition. We would use this on the basis of legitimate business interests.