HBL Belgium Branch Personal Data Protection Statement for Customers

19 February 2024

Contents

1. Who we are:

This Personal Data Protection Statement (referred hereby also as "Privacy Statement") applies to all Personal Data information (see section "What is Personal Data" for a description of what this means) processing activities carried out by HBL Belgium Branch in connection with delivery of services to clients and prospects.

Habib Bank Limited Belgium Branch (trading as "HBL Belgium"), registration number: BE 0415.466.440, is a data controller in respect of Personal Data that we process in connection with our business (including the products and services that we provide). In this Privacy Statement, references to "we", "us" or "our" are references to HBL Belgium.

HBL Belgium is branch of HABIB BANK LIMITED, a banking company established under the laws of Islamic Republic of Pakistan and having its head office at HBL Plaza, I. I. Chundrigar Road, Karachi, Pakistan, ("HBL").

Our principal address is Troonstraat / Rue du Trône 14-16, 1000 Brussels, Belgium. We're reachable via email at: brussels.dpo@hbl.com and via phone at: 0032 2 286 5960. Please use these contact details if you wish to contact us in relation to any of the matters mentioned in this Privacy Statement.

2. Purpose of this Privacy Statement:

The purpose of this Privacy Statement is to explain how we collect and use Personal Data in connection with our business. In addition, we explain your rights under applicable data protection law.

We are committed to protecting your Personal Data from unauthorised access, use and disclosure.

3. Who are subject to this Privacy Statement:

This Privacy Statement refers and applies to you if you are or was:

- one of HBL Belgium Branch customers (current and past customers);
- a prospect as person or entity interested in our products or services when you provide us with your Personal Data (in an agency or by email) so that we can contact you and establish a business relationship;
- in a business relationship with us (e.g., trade finance related party or lender in a syndicated loan or borrower);
- a member of our customer's family and/or household. Indeed, our customers may occasionally share with us information about their family when it is necessary to provide them with a product or service;
- a legal representative of our customers or prospects;
- an authorised individual representing our customer or prospects;
- a beneficiary of a payment made by our customers;
- a remitter of a payment sent to our customers;
- a beneficial owner of our customers or prospects;
- a debtor (e.g. in case of bankruptcy of our customers);
- a shareholder of our customers or prospects;
- a member of our customer's staff.

All data subjects in scope of this Privacy Statement and defined in this section are referred as customers in general for the purpose of this Privacy Statement.

When you provide us with Personal Data related to other people, please make sure that you inform them about the disclosure of their Personal Data and invite them to read this Privacy Statement.

4. What is Personal Data and where do we get it from:

When we refer to Personal Data, Personal Data or simply information, we mean information about a living individual who can be identified from that information, either by itself or when it is combined with other information. Personal Data includes (by way of example only):

- basic personal information including name, address, date of birth and contact details;
- financial information including account and transactional information and history;
- information about your family, lifestyle and social circumstances (such as dependents, marital status, next of kin and contact details);
- information about your financial circumstances including personal wealth, assets and liabilities, proof of income and expenditure, credit and borrowing history and needs and goals;
- education and employment information;
- services provided;
- visual images and personal appearance (such as copies of passports or CCTV images); and
- online profile based on your interaction with us, our websites and applications, including for example, your banking profile and login information, Internet Protocol (IP) address, smart device information, location coordinates, online and mobile banking security authentication, mobile phone network information, searches, site visits and spending patterns.

Your Personal Data is made up of all the financial and personal information we collect and hold about you/ your business and information about the proprietors, officials, directors and beneficial owners of that business, and your transactions. It includes:

- information you give to us;
- information that we receive from third parties including third parties who provide services to you or us, and credit reference, fraud prevention or government agencies, and other banks (where permitted by law);
- information that we learn about you through our relationship with you and the way you operate your accounts and/ or services, such as the payments made to and from your accounts;
- information that we gather from the technology which you use to access our services (for example location data from your mobile phone, or an IP address or telephone number) and how you use it (for example pattern recognition); and
- information that we gather from publicly available sources such as the press, the electoral register, company registers and online search engines.

5. The information we process:

We collect and process various categories of Personal Data at the commencement of and for the duration of your relationship with us. We will limit the collection and processing of information to information necessary to achieve one or more legitimate purposes as identified in this Privacy Statement.

5.1 When you wish to become our client (client onboarding/ prospect):

Before we're able to provide services to you, we would need to take steps related to verifying your/your business' identity and running certain due diligence checks on you. This may include verification of customer identity through various sources such as official databases, third-party providers, in addition to collecting ID documents. Further, we would need to assess every customer's risk profile.

If you wish to become our client, we will usually collect the following Personal Data: A copy of your ID document(s), income information, private address, full name, date and location of birth, nationality, government-issued identification numbers such as social security number, financial data, phone number - private and professional, signature, credit or debit card number, professional activities, gender, marital status, any public mandates, children, husband or wife names, accommodation details (address, rented or owned, rent, charges etc.),

professional experience, employer name, job role, recruitment date, work location, reason and date of end of employment contract, and wages.

Such Personal Data is collected for the following purpose(s): so that we are able to provide you with our services, while complying with our Know Your Customer procedures.

In order to process such Personal Data, we rely on the following legal base(s): taking steps to enter into a contract for services with you (art 6.1.b GDPR); compliance with our legal obligations as a regulated financial institution (art 6.1.c GDPR); pursuing our legitimate interests that are to guarantee the safety of the assets of our business and to protect its officers from prosecution (art 6.1.f GDPR). In addition, in specific circumstances, we process your data if you have given your explicit consent. In such circumstances, as per your rights you can withdraw your consent at any time.

5.2 Once you are a client (client operations):

Following satisfaction of the onboarding verifications we need to conduct to onboard you/your business as our client and once we formally accept you as a such, we would be ready to provide you with banking services. The information we would process in connection with the provision of our services depends on the exact service at hand. For example, we may need to record information related to various financial transactions, such as deposits, withdrawals, transfers, loan payments, etc. On the other hand, if you apply for a loan through us, we would be recording information provided by you, such as income details, employment information, credit history, and any other relevant financial information required for the loan evaluation and approval process. During the time you're a client we would also need to communicate with each other, and this may often involve the exchange of Personal Data.

To provide you with our services, depending on the operation at hand, we would need to process some or all of the following Personal Data: (a) all the information you have provided in order to become a client and (b) further information such as: customer ID, customer (risk) profile, transaction history, income/revenue, bank account details, transaction history, savings, investments, loans, insurance types, pension details, transactions data, credit or debit card number, usernames, passwords, security questions, account analytics and reporting and other categories of information you disclose or generate.

Such Personal Data is used for the following purpose(s):

- account operations and the receipt of financial services, current account, loans, funds settlement and clearance, financial statement preparation and reporting to you, customer relationship management, national and international transactions processing, including currency exchange, borrowing services, managing your access to our online systems, inquiries and complains handling, provision of personalised services.
- account maintenance and analytics which involve collecting and analysing customer account data to generate reports, insights, and analytics for internal purposes, such as enhancing customer experience, detecting fraud and suspicious activity and reporting the same; and assessing business performance.
- Euro clearing which involves communication with clearinghouses or central counterparties and maintaining communication logs for the purpose of international transactions.

This list of purposes may not be exhaustive. While you are our client you may request us to process your information for other purposes in connection with specific services. Where that is the case, you would know what Personal Data we process, because you would submit it in connection with your specific request. Nevertheless, the aforementioned purposes are the three key processing operations that we expect to carry out in connection with the delivery of all core banking services.

In order to process such Personal Data, we rely on the following legal base(s): the performance of the contract between us and you (art 6.1.b GDPR); pursuing our legitimate interests that are to develop and improve our services (art 6.1.f GDPR).

5.3. Periodic monitoring, risk management and fraud prevention:

We may access and use information from credit reference and fraud prevention agencies and share information with them when you open your account and periodically thereafter, in order to manage and take decisions about your accounts, including assessing your creditworthiness and checks to avoid customers becoming over-indebted; prevent criminal activity, fraud and money laundering; check your identity and verify the accuracy of the information you provide to us; trace debtors and recover debts, etc. A customer profile risk assessment is conducted to ensure compliance with regulations like anti-money laundering (AML) and counter-terrorism financing (CTF). This involves evaluating the risk associated with each customer account. As a regulated financial institution, we obliged to carry out certain monitoring activities to manage risk in accordance with the law and to take measures to prevent fraud, money laundering and terrorist financing. To that end, we will monitor your transactions including their amounts and types to identify suspicious or fraudulent activities. We create logs of customer authentication activities, such as login attempts, password changes, and account access, to identify any unauthorised access attempts. We are tracking and documenting account activities, such as balance inquiries, fund transfers, and withdrawals, to detect any unusual or suspicious transactions. Where our monitoring processes reveal suspicious or criminal activity, we will pass on relevant information to law enforcement agencies and regulatory bodies.

To that end, we will collect the following Personal Data: all information you've provided to us including the information mentioned in the preceding paragraph.

Such Personal Data is collected for the following purpose(s): for security purposes, fraud prevention and investigation purposes and compliance purposes.

In order to process such Personal Data, we rely on the following legal base(s): our legitimate interests, that are to ensure fraud prevention and the safety and security of our clients and members of staff and to protect our assets (art 6.1.f. GDPR); and compliance with our legal obligations connected to fraud prevention and production of evidence, suspicious activity monitoring and reporting, whistle blowing management, etc (art 6.1.c. GDPR). The monitoring of transactions and other AML-related monitoring and data collection are in scope of the Belgian AML Law of 18 September 2017.

5.4 Managing recordings:

We may monitor and record various forms of communication between us and you including calls, emails and text messages via various channels, as well as video recordings captured by our CCTV system during visits to our branches, always with prior notice to you. We may do this in the following situations and as follows:

- CCTV Recordings: Our branches are equipped with video surveillance (CCTV) to ensure the safety and security of our clients, staff members, and assets. Video footage from our CCTV system is retained for a duration of 30 days.
- Calls Recordings: We may record communications via the phone with you for production of evidence, fraud prevention, and investigation and compliance purposes, at all times with prior notice to you. Call recordings are kept for 10 years.
- Email Communications Monitoring: In the case of email communications, records may be maintained for up to 10 years after the termination of the customer relationship. This extended period is aligned with our commitment to meeting legal obligations and preserving communication history.

In order to process such Personal Data, we rely on the following legal base(s): our legitimate interests, that are to ensure fraud prevention and the safety and security of our clients and members of staff and to protect our assets (art 6.1.f. GDPR); and compliance with our legal obligations connected to fraud prevention and production of evidence (art 6.1.c. GDPR).

5.5 When you visit our website:

When you visit our website, certain information technical information is transmitted to us from your device, either at your direction or through the use of tracking technologies such as "cookies". A cookie is a piece of information

that is deposited by our computer server when you visit our website, which is stored on your computer's hard drive by your web browser. On revisiting this website, our computer server will recognize the cookies, giving us information about your last visit. Most browsers accept cookies automatically, but usually you can alter the settings of your browser to prevent automatic acceptance. You can learn more about cookies by visiting our cookies policy.

When you visit our website, we will usually collect the following Personal Data: your banking profile and login information, Internet Protocol (IP) address, device information, location coordinates, mobile phone network information, searches, site visits, spending patterns, etc.

Such Personal Data is collected for the following purpose(s): to deliver our services online, to ensure the proper functioning of our website(s) and to improve our website(s).

In order to process such Personal Data, we rely on the following legal base(s): when the processing is in connection with the delivery of our services, it is necessary for the performance of the contract between us and you (Art 6.1.b. GDPR); when the processing is in connection with ensuring the proper functioning of our website(s), it is necessary for the pursuit of our legitimate interests, that are to deliver a running and safe online service (art 6.1.f. GDPR); when the processing is in connection with improving our online services, it is subject to your consent when required by law, or where that is not required, it is necessary for the pursuit of our legitimate interests, that are to improve our online services(art 6.1.f. GDPR).

6. Disclosing your information within the HBL and to other parties:

We will only use and share your information where it is necessary for us to lawfully carry out our business activities. Your information will be shared with and processed by HBL and its subsidiaries/entities for the purposes stated in this Privacy Statement. We will not share your information with anyone outside the HBL except when any of the following conditions applies:

- where we have your permission;
- where required for your product or service requested by you;
- where we are required by law and/or by law enforcement agencies, courts and judicial authorities, government entities, tax authorities or regulatory bodies around the world;
- with other banks and payment institutions where required by law to help recover funds that have been credited to your account in error;
- with third parties providing services to us, such as correspondent banks processing payments,;
- with other banks or payment institutions to facilitate investigations where you are a victim of suspected fraud and you have agreed for us to do so, or where we suspect funds have been credited to your account as a result of a financial crime;
- with debt collection authorities in Belgium;
- with credit reference and fraud prevention authorities in Belgium;
- where required for a proposed sale, re-organisation, transfer, financial arrangement, asset disposal or other transaction relating to our business and/or assets held by our business;
- in anonymised form as part of aggregated data for statistical or reporting purposes to our head office or Belgium Authorities; or
- where permitted by law, it is necessary for the protection of our legitimate interests or those of a third party.

If any additional authorised users are added to your account, we may share information about the use of the account by any authorised user with all other authorised users. If you ask us to, we will share information with any third party that provides you with account information or payment services. If you ask a third-party provider to provide you with account information or payment services, you are allowing that third party to access information relating to your account at HBL Belgium Branch. We are not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any Privacy Statement they provide to you.

7. Transferring information outside of Belgium:

Some of the data we collect from you will be transferred to and stored with organisations (including HBL), third party suppliers and agents at a destination(s) outside Belgium and the European Economic Area. Where we engage in such overseas transfers we will only do so where:

- the European Commission has decided that the country or the organisation we are sharing your information with will protect your information adequately; or
- we have entered into a contract with the organisation with which we are sharing your information (on terms approved by the European Commission) to ensure your information is adequately protected; or
- the organisation we're sharing your information with participates in a valid scheme or certification enabling lawful transfers under Chapter V of the GDPR such as the EU-US Data Privacy Framework.

8. How long do we keep your Personal Data for:

By providing you with products or services, we are legally required to create records that contain your information, such as customer account records, activity records, tax records, lending and credit account records, information that we gather from technology which you use to access our services (for example IP address, location data from your phone), and information we gather from public sources such as the press, the electoral register, company register and online search engines. Records can be held on a variety of media (physical or electronic) and in different formats. We manage our records to help us to serve our customers better and to comply with legal and regulatory requirements. Records help us demonstrate that we are meeting our responsibilities and to archive as evidence of our business activities in the event of future disputes that require the bank to provide transactional and other information to the courts. We may by exception retain your information for longer periods, particularly where we need to withhold destruction or disposal based on an order from the courts or an investigation by law enforcement agencies or our regulators. This is intended to make sure that the bank will be able to produce records as evidence, if they are needed.

Retention periods for records are determined by the type of record, the nature of the activity, product or service and the applicable local legal or regulatory requirements. We normally keep customer account records for up to seven years after a customer relationship with the bank ends, whilst other records are retained for shorter periods, for example CCTV records and call recordings are kept for shorter durations. Retention periods may be changed from time to time based on business or legal and regulatory requirements. For specific retention periods in respect of specific records, please contact us using the details provided above.

9. Your rights:

If you wish to exercise any of your rights under data protection law, if you have any queries about how we use your Personal Data that are not answered here, or if you wish to complain about our data handling processes, please contact us using the details provided above. You have the following rights in respect of your information.

9.1 Right to Information

The right to obtain clear, transparent and comprehensible information about how we process your Personal Data and how to exercise your rights. This information is contained in this Privacy Statement. If this information is not clear enough, please contact us using our contact details in the Privacy Statement.

9.2 Right of Access

The right to get access to the Personal Data we hold about you. If you would like a copy of the Personal Data we hold about you, please write to us using the contact details provided in this Privacy Statement.

9.3 Right to Rectification

The right to correct/rectify inaccurate Personal Data and to update incomplete Personal Data. If you believe that any of the information that we hold about you is inaccurate, you have a right to request or restrict the processing of that information and to rectify the inaccurate Personal Data. To exercise this right, you may contact us using the contact

details provided in this Privacy Statement, clearly specifying the reasons why you think the data should be corrected and attaching any documents that show this to be the case. If we correct your Personal Data which we have previously shared with a third party, we will also notify the third party.
Please note that if you request us to restrict processing your Personal Data then we may have to suspend the operation of your account and/or products and services we provide to you.

9.4 Right to be Forgotten
The right to request that we delete your Personal Data. You may request that we delete your Personal Data if you believe that we no longer need to process your information for the purpose it was provided or you have withdrawn your consent or we are not using it in a lawful way (subject to the Bank not having a legal obligation or statutory or legal obligations to retain that information for a certain period of time). Please note that if you request us to delete your information, we may have to suspend the operation of your account and/or the products and services we provide to you.

9.5 Right to Restriction
The right to request us to restrict the processing of your Personal Data. You may request us to restrict processing your Personal Data if you believe that any information we hold may be inaccurate, or we no longer need to process your information for the purposes for which it was provided or we are not using your information in a lawful manner. Please note that if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.

9.6 Right to data Portability
Where we have requested your permission to process your Personal Data or you have provided us with information for the purposes of entering into a contract with us, you have a right to receive the Personal Data you provided to us in a portable format where it is technically feasible. For example, you may request us to provide it directly to a third-party aggregator, if technically feasible. We are not responsible for any such third party's use of your Personal Data information, and any breach of confidentiality, or misuse of this information for identity theft, which will be at your own risk and responsibility, and will be governed by their agreement with you and any Personal Data Privacy Statement or Policy they provide to you.

9.7 Right to Withdraw Consent
Where we rely on your permission to process your Personal Data, you have a right to withdraw your consent at any time. We will always make it clear where we need your permission to undertake specific processing activities. However, withdrawing your consent does not call into question the legality of the processing carried out during the period before you withdrew your consent.

9.8 Right to Objection
You have a right to object to us processing your Personal Data unless we can demonstrate compelling and legitimate grounds for the processing, which may override your own interests or where we need to process your information to investigate potential fraud, illicit or unlawful activities, including but not restricted to money laundering, sanctions screening, tax evasion, preventing financing of terrorism and to protect the Bank or others from legal claims. Depending on the circumstances, we may need to restrict or cease processing your Personal Data altogether or, where requested, delete your information.
Please note that if you object to us processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.

9.9 Right to Object for Marketing purposes
HBL Belgium does not conduct marketing campaigns on their products and services through any form or medium. In the case that this changes in the future, you will be notified, and you will have the right to object at any time to processing of your Personal Data for direct marketing purposes. You will also have a right to withdraw your consent at any time without justification and at no cost. You will be able to do so by contacting your branch relationship manager or contact person or us using the contact details provided in this Privacy Statement.

10. Changes to this Privacy Statement:

We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes Personal Data. This version was published at the end of February 2024 and enters into force on 1st April 2024. The most recent version is available at https://www.hbl.com/Belgium/. We invite you to frequently check the website to see the version of the Privacy Statement currently in force.

Where we believe you may not reasonably expect a significant change to how we process your Personal Data, we will notify you through the channel of communication your provided to us and will allow a period of at least 30 days for you to raise any objections before the change is made. However, please note that in some cases, if you do not agree to such changes, it may not be possible for us to continue to operate your account, maintain our business relationship and/or provide certain products and services to you.

11. Questions, requests and making a complaint:

If you wish to exercise your rights, if you have questions about this Privacy Statement or if you have any concerns about the way we process your Personal Data or are not happy with the way we have dealt with any request from you then you may contact our Data Protection Officer via email at brussels.dpo@hbl.com who will investigate the matter. We hope we can address any concerns that you may have.

12. Complaints to the Data Protection Authority:

You have the right to complain about our Personal Data processing activities to the Data Protection Authority (DPA) in Belgium (in French: Autorité de protection des données (APD), and in Dutch: Gegevensbeschermingsautoriteit (GBA)). Below are their contact details:

Address: Rue de la Presse 35 / Drukpersstraat 35 1000
Bruxelles / Brussel
BELGIUM
Webpage: http://www.dataprotectionauthority.be
Email: contact@apd-gba.be
Phone: +32 2 274 48 00
Company Number: 0694.679.950

*
* *