



DATA PRIVACY POLICY

CONFIDENTIALITY

No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of KEYSTONE BANK LIMITED. This document, its associated appendices and any attachments remain the property of KBL LTD and shall be returned upon request



Document Control Sheet

Document Ref	DATA PRIVACY POLICY
Origin	Compliance Division
Document Owner	Keystone Bank Limited
Document Classification	Confidential/Internal/Restricted
Document Status	Approved
Date Signed Off	MARCH 17, 2020
Next Review Date	MARCH 16, 2023

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
N/A	N/A	N/A	N/A

*The sign-off of this document by all stakeholders authorizes the immediate implementation of **DATA PRIVACY POLICY** at Keystone Bank Limited*

Change Control

The contents of this document are subject to change control.





TITLE:	PRIVACY STATEMENT
---------------	--------------------------

1.1. Introduction:

- This privacy notice explains how Keystone Bank Limited (KBL) collects and uses personal data, and describes the rights you have with respect to your personal data.
- In this notice, “KBL,” “our”, “we” or “us” refers to Keystone Bank Limited and its Subsidiaries, each of which is a separate legal entity. The controllers of your personal data are one or more of the KBL entities which include Global Bank Liberia, Keystone Bank Sierra Leon and KBL Insurance.
- KBL processes personal data for a variety of purposes. We collect this personal data directly from you, for example, if you are on-boarded as our customers, vendors, consultants, job applicants etc., if you visit **www.keystonebankng.com** (our website), if you submit your contact details to receive marketing communications from us, if you visit our Head office and branches or submit a job application via the KBL careers website. Alternatively, we process your personal data in the context of providing financial services to your employer/employee or service provider, for example, remittance of payroll for the company you work for. Finally, we obtain your personal data via publicly available sources, such as LinkedIn. This privacy notice is intended to cover all and many more scenarios.

Below are the more detailed information regarding various purposes for which we process personal data:

- Visitors to www.keystonebankng.com
- Customers/Staff/Vendor
- Individuals whose personal data we obtain in connection with providing services to our customers
- Contacts in our banking application systems
- Participants of KBL meetings, conferences, events and learning sessions
- Individuals who use our applications
- Individuals who visit our social media sites, social media plugins and tools
- Individuals who correspond with KBL via email/contact center
- Job applicants
- Alumni
- Vendor/Suppliers
- KBL/Ethics
- Visitors to KBL offices

If you have any questions regarding the processing of your personal data or wish to contact the Data Protection Officer of Keystone Bank Limited, please contact the KBL Data Protection Team who will direct your query to the appropriate person or team within the Bank.



1.2. Which data are covered?

In this privacy notice, “personal data” means any information relating to an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, Date of Birth, location data or an online identifier. Personal data also refers to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual.

It also includes special categories of personal data (special category data) from which we can determine or infer an individual's

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Membership of a trade union
- Genetic data
- Biometric data
- Physical or mental health or condition
- Sex life or sexual orientation

As well as personal data relating to criminal convictions and offenses.

1.3. Your rights in relation to personal data

You have the following rights in relation to your personal data:

- To access the personal data held by KBL about you
- To have your personal data corrected, for example, if it is incomplete or incorrect.
- To opt out of receiving marketing communications at any time
- To restrict or object to the processing of personal data or request erasing personal data (in certain circumstances and subject to applicable law)
- To receive a copy of the personal data which you have provided to KBL, in a structured, commonly used and machine-readable format (known as “data portability”) (in certain circumstances and subject to applicable law)
- Where you have provided personal data voluntarily, or otherwise consented to its use, the right to withdraw your consent
- The right to complain to a data protection authority (see section “Complaints ”)

If you have a query or wish to exercise your rights, please speak to the person you usually deal with at KBL or contact the KBL Data Protection Team.

1.4. Complaints

- If you are concerned about an alleged breach of privacy law or any other regulation by KBL, you can contact the person you usually deal with



(Relationship Manager) or Contact KBL Head office at 1 Keystone Bank Crescent Victoria Island, Lagos and at any of our branches nationwide. KBL Data Protection Officer will investigate your complaint and give you information about how it will be handled.

- You also have the right to complain to the data protection authority in Nigeria - NITDA, or refer the matter to a court of competent jurisdiction or as specified in any applicable engagement agreement with KBL.

2.1.0 Purpose for Which We Process Personal Data

2.1.1 Visitors to Keystone

Personal data that we collect about you when you visit our site falls into several categories.

2.1.2 Information that you provide voluntarily

We collect personal data that you provide voluntarily through our site or when opening account through our channels, for example, when you are on-boarded as customer/staff/vendor, when completing online forms to open account, contact us, subscribing to a newsletter, using one of our online benchmark tools, subscribing to receive marketing communications from us, participating in surveys or registering for events that we are organizing. The information we collect about you include the following:

- Name
- Job title, job level or job function, role
- Company or organization
- Company data
- Contact information, including primary email, email address and telephone numbers
- Demographic information, such as industry, country, postcode, preferences and interests
- Other information relevant to customer surveys or similar research
- Information pertinent to fulfilling our services to you
- Any other personal data that you voluntarily choose to provide to us

We do not intentionally collect sensitive category data, unless you provide us with such data. While there may be free text boxes on the site where you are able to enter any information, we do not intend to process sensitive information. You are not required to provide, and should not disclose, sensitive personal information in the free text boxes. If you choose to provide any sensitive personal information in this manner, you acknowledge you consent to the collection and processing of this sensitive information.



If you register on our site, your personal data will be stored in our Banking Application systems. If you have opted out of receiving KBL publications, your basic contact details will remain on our opt-out list.

2.1.3 Information that we collect automatically

When you visit our site, we collect certain personal data automatically from your device. Specifically, the data we collect automatically include information, such as your IP address, device type, unique device identification number, browser type, broad geographic location (e.g., country or city-level location) and other technical information. We also collect information about how your device has interacted with our site, including the pages accessed and links clicked. Collecting this information enables us to better understand the visitors who come to our site, where they come from and what content on our site is of interest to them. We use this information for our internal analytics purposes, and to improve the quality and relevance of our site to our visitors. Information will be collected using cookies and similar tracking technology, as explained further in the KBL Cookie Policy.

Our site also uses various social media plugins.

2.1.4 Purposes for which we process your personal data as a visitor to our site are:

- To administer and manage our site, including to confirm and authenticate your identity, and prevent unauthorized access to restricted areas of our site.
- To personalize and enrich your browsing experience by displaying content that is more likely to be relevant and of interest to you
- To analyze the data of visitors to our site
- To determine the company, organization, institution or agency that you work for or with which you are otherwise associated
- To develop our business and services
- To provide you with marketing communications, KBL materials and online benchmarking tools
- To conduct benchmarking and data analysis (for example, regarding usage of our site and demographic analyses of visitors of our site)
- To understand how visitors use the features and functions of our site
- To monitor and enforce compliance with applicable terms of use
- To conduct quality and risk management reviews
- Any other purpose for which you provided information to KBL.

2.1.5 Legal grounds for processing personal data of visitors of our site are:

- Our legitimate interest in the effective delivery of information and services to you, and the effective and lawful operation of our business
- Our legitimate interest in developing and improving our site, and your user experience
- Explicit consent of the visitor



2.2.0 Customers/Staff/Vendor

When you engage us to provide you with financial services to Customers/Staff/Vendor, we collect and use personal data when we have a valid business reason to do so in connection with those services.

In the context of providing financial services to Customers/ Staff/Vendor, KBL also processes personal data of individuals who are not directly our Customers/Staff/Vendor (for example, employees, customers or suppliers of our Customers/Staff/Vendor). See the section "Individuals whose personal data we obtain in connection with providing services to our Customers/Staff/Vendor" for additional information.

The majority of the personal data we collect and use to provide our services is supplied voluntarily by (or collected by us from third-party sources at the request of) our Customers/Staff/Vendor. Because of this, if you are a Customers/Staff/Vendor of KBL, then it will generally be obvious to you what personal data we collect and use. This information can include:

- Basic information, such as your name, the company you work for, your position and your relationship to a person.
- Contact information, such as your postal address, email address and telephone numbers.
- Financial information, such as payment-related information.
- Any other personal data relating to you or other third parties which you provide to us for the purpose of receiving our services.

We use this information:

- To provide services to you.
- To administer our relationship and maintain contractual relations.
- For accounting and tax purposes.
- For marketing and business development.
- To comply with our legal and regulatory obligations.
- To establish, exercise or defend legal rights.
- For historical and statistical purposes.

Given the diversity of the services we provide, we process many categories of personal data. Please see below (non-exhaustive) examples of personal data categories for our four main service lines:

2.2.1 Financial Services

In providing account opening and financial services, KBL will process information that contains personal data, such as board records and other documents attributable to aid Customers/Staff/Vendor and any group companies' activities. Examples of categories of personal data that are processed are:



- Personal Data such as Name, Date of Birth, Sex, Origin and Biometric information
- Contact details, such as address, telephone numbers and email address
- Details of employment, such as employer name, role and employment time
- To administer and manage our site, including to confirm and authenticate your identity, and prevent unauthorized access to restricted areas of our site
- To personalize and enrich your browsing experience by displaying content that is more likely to be relevant and of interest to you
- To analyze the data of visitors to our site
- To determine the company, organization, institution or agency that you work for or with which you are otherwise associated
- To develop our business and services
- To provide you with marketing communications, KBL materials and online benchmarking tools
- To conduct benchmarking and data analysis (for example, regarding usage of our site and demographic analyses of visitors of our site)
- To understand how visitors use the features and functions of our site
- To monitor and enforce compliance with applicable terms of use
- To conduct quality and risk management reviews
- Any other purpose for which you provided information to KBL

2.2.2 Trade Finance

In providing trade finance, we understand that no two businesses are the same, therefore we provide services to fit dynamic trade finance needs and unique backgrounds. KBL will process information that contains personal data, such as trade records and other documents attributable to the aid Customers/Staff/Vendor and any group companies' activities. Examples of personal data categories processed by KBL for trade finance purposes on behalf of Customers/Staff/Vendor include:

- Personal details for the individual Customers/Staff/Vendor names, addresses and demographic, contact information, dates of birth, and tax identifiers, including social security numbers and email addresses
- Personal details for the individual Customers/Staff/Vendor delegates, including names, contact information and email addresses
- Current, past or future travel information for the individual, including locations visited and workday activities that occurred in each location
- To administer and manage our site, including to confirm and authenticate your identity, and prevent unauthorized access to restricted areas of our site
- To personalize and enrich your browsing experience by displaying content that is more likely to be relevant and of interest to you
- To analyze the data of visitors to our site
- To determine the company, organization, institution or agency that you work for or with which you are otherwise associated
- To develop our business and services



- To provide you with marketing communications, KBL materials and online benchmarking tools
- To conduct benchmarking and data analysis (for example, regarding usage of our site and demographic analyses of visitors of our site)
- To understand how visitors use the features and functions of our site
- To monitor and enforce compliance with applicable terms of use
- To conduct quality and risk management reviews
- Any other purpose for which you provided information to KBL

2.2.3 Loans and Advances

In providing loans and advances, KBL processes a wide variety of information, including potentially all types of personal data. The scope depends on the service and the sector in which the customer is active. For example, providing loan and advances to customer involves the processing of different types of personal data which include third parties information such as the guarantors.

Examples of personal data categories received or processed by Loans and Advances teams are:

- Contact details, such as name, address, telephone numbers and email address
- Guarantor records of customers, which include personal name, contact details, date of birth, race, government identification numbers, employment contracts and service contracts
- Financial data, such as wage and salary information, pension and retirement benefits information, and bank account numbers

2.2.4 Transaction Advisory Services

In addition, we also process identification and background information as part of our customer acceptance, finance, administration and marketing processes, including anti-money laundering, conflicts, reputational and financial checks, and to fulfill any other legal or regulatory requirements to which we are subject.

The checks could include the following:

- Identity verification: proof of name and address
- Ultimate beneficial ownership of corporate and other legal entities
- Conflicts checks: to avoid a conflict of interest with any other customer
- Anti-Money Laundering (AML), proceeds of crime and terrorist financing checks
- Politically Exposed Persons (PEP) checks: those with prominent roles in government, judiciary, courts, central banks, embassies, armed forces and state-owned enterprises, including their family members and close associates
- Adverse media checks
- Government sanctions list checks
- Independence checks



These checks are made for legal, regulatory or business reasons and need to be repeated during the course of the relationship. As part of these checks, we are required to process special category data (for example, to verify if you are a politically exposed person or to collect information about criminal convictions where this is required for anti-money laundering laws). It is important you provide us with all necessary information and documents as this affects our ability to provide services to you.

2.2.5 Legal grounds for processing personal data of our customers are:

Performance of a contract

- Compliance with a legal or regulatory obligation
- Our legitimate interest in providing you with seamless, consistent, high-quality services and securing prompt payment of any fees, costs and debts in respect of our services
- Our legitimate interest in understanding any conflict of interest or challenge with regard to independence legislation
- Our legitimate interest in safeguarding KBL against inadvertently dealing with the proceeds of criminal activities or assisting in any other unlawful or fraudulent activities (for example, terrorism)

2.3.0. Individuals Whose Personal Data we obtain in connection with providing services to our customers

As part of the financial Intermediary services KBL provides to Customers/Staff/Vendor, KBL processes personal data of individuals with whom we do not have a direct (contractual or other) relationship. For example, if we avail loans to our customers, our engagement team will be required to, review the financial administration, data regarding guarantors and legal proceedings. To take another example: if we undertake a due diligence review of a customer, KBL obtains personal data concerning the target's customers.

We seek confirmation from our Customers/Staff/Vendor that they have the authority to provide personal data to us in connection with the performance of the services and that any personal data they provide to us has been processed in accordance with applicable law.

Given the diversity of services we provide, we process many categories of personal data such as:

- Personal details (such as name, age, data of birth, gender, marital status and country)
- Contact details (such as phone numbers, email address and postal address)



- Financial details (such as salary, payroll, income, investments, benefits and tax status)
- Employees details (such as role, rank, experience, performance data and employment numbers)

For certain services, we also process special category data. For example, in certain countries performing tax return services involves the processing of details of payments made by our customer, his or her spouse and dependents with respect to a trade union membership, to a political party, for medical treatments or to a religious charity. Such data is collected intentionally and will be used only where necessary in connection with the provision of the service for which the data was collected,

2.3.1 Legal grounds for processing personal data of individuals whose personal data we obtain in connection with providing services to our customers are:

- Compliance with a legal or regulatory obligation
- Our legitimate interest in making sure our customers are provided with seamless, consistent and high-quality services worldwide

2.4.0 Contacts in our Banking Application System

We process personal data about contacts (former, existing and potential customers and individuals employed by, or associated with, such customers and other business contacts, such as consultants, regulators and journalists) in our banking applications. These systems support the business and marketing operations of KBL. Contacts in our banking applications may be sent KBL newsletters, marketing materials, learning opportunities, reactivation of accounts, surveys and invitations to events.

In our systems, we process the following categories of personal data:

- Name, job title, address, email address, phone and fax numbers
- Name of employer or organization the individual is associated with
- Marketing preferences
- Invitation responses and event attendance confirmations

We do not intentionally collect sensitive category data, unless you provide us with such data (for example, special dietary requirements which reveal your religious affiliation or any food allergies), if you attend one of our events.

Data of business contacts who have not been actively engaged with KBL will be kept in line with relevant laws in Nigeria. If you have opted out of receiving future KBL publications, your basic contact details will remain on our opt-out list.

2.4.1 Legal grounds for processing personal data of business contacts are:

- Explicit consent of the business contact



- Our legitimate interest in managing the relationship with our business contacts and providing information about KBL, our services and events we organize

2.5.0 Participants in KBL Meetings, Conferences, Events and learning sessions

We process personal data about participants in KBL meetings, conferences, events and learning sessions (events). We use various applications to manage event registration processes, which applications will contain their own privacy notices explaining why and how personal data is collected and processed by these applications. We encourage participants to refer to the privacy notices available on those applications.

As part of our event management processes, we process the following personal data (but only to the extent required for a specific event):

- Name, age or date of birth
- Customer personnel information (home, office, and business information)
- Credit or debit card number
- Customer information (home, office and business information)
- Email address
- Gender
- Home or other physical address
- Names of employers (KBL or company)
- Occupation (job title)
- Passport number
- Personal web URL (if you have a personal website that you would like to share)
- Telephone or fax numbers

We do not intentionally collect sensitive category data, unless you provide us with such data (for example, special dietary requirements which reveal your religious affiliation or any food allergies or other data relating to your health necessary to provide support to participants, if needed, for example, if a wheelchair will be required).

Attendees of KBL events hosted at external venues are required to bring a photo ID for identification purposes to safeguard our people, assets and information, and to prevent unauthorized people gaining access to off-site KBL events.

KBL is allowed to take photographs and make audio or video recordings in public areas of the KBL events. We use such media in our marketing materials. Images and voices of attendees will be recorded. Recordings will be edited, copied, exhibited, published or distributed.

2.5.1 Legal grounds for processing personal data of participants are:



- Explicit consent of the participant
- Our legitimate interest in organizing events and managing the registration process for such events
- Our legitimate interest in protecting our people, assets and information, and to prevent unauthorized people gaining access to off-site KBL events
- Our legitimate interest in providing information about KBL, our services and events we organize

2.6.0 Individuals who use our applications

We provide external users access to various applications managed by the bank. In instances where such applications process personal data that goes beyond basic contact information used for application authentication purposes, such applications will contain their own privacy notices explaining why and how personal data is collected and processed by those applications. We encourage individuals using our applications to refer to the privacy notices available on those applications.

2.7.0 Individuals who visit our social media sites, social media plugins and tools

2.7.1 Social Media Sites

KBL uses various social media platforms, for example, for recruitment or marketing purposes. We use social media to provide you with easy access to relevant information regarding financial opportunities at KBL and events we organize, and to promote our services and brand.

While KBL will be responsible for the content it publishes using social media platforms, KBL will not be responsible for managing the social media platforms (such as creating user statistics or placing cookies). When using these social media platforms, you are obliged to adhere to the legal and privacy terms imposed by the social media platform providers. Such providers collect personal data about you, including statistical and analytical data regarding your use of the social media platforms, such as an overview of pages you have accessed, “likes,” recent visits, posts you publish or find interesting. If you require access to such data or want to invoke one of your other rights (such as the right to object to the processing of your data), you should contact the social media platform provider. Some social media providers provide KBL with aggregate data relevant for our pages, such as the amount of “likes” triggered by our content or the amount of posts, visitors to our sites, photos that are downloaded or links that are clicked.

2.7.2 Social Media Plugins (such as like and share buttons)

On our site, we implement so-called social media plugins. When you visit a page that displays one or more of such buttons, your browser will establish a direct connection to the relevant social network server and load the button from there. At the same time, the social media provider will know that the respective page on our site has been visited. We have no influence on the data that the social media



providers collect on the basis of the buttons. If you wish to prevent this, please log out of your social media accounts before visiting our website. Social media providers set cookies as well, unless you have disabled the acceptance and storage of cookies in your browser settings.

2.7.3 Facebook plugins

Our site includes plugins for the social network, Facebook. The Facebook plugins can be recognized by the Facebook logo or by the like button on our sites.

When you visit our site, a direct connection between your browser and the Facebook server is established via the plugin. This enables Facebook to receive information that you have visited our site from your IP address. If you click on the Facebook "like button" while you are logged into your Facebook account, you can link the content of our site to your Facebook profile. This allows Facebook to associate visits to our site with your user account. If you are not yet logged into your Facebook account, clicking a Facebook button will show you the Facebook login page for you to enter your login credentials. Please note that we have no knowledge of the content of the data transmitted to Facebook or of how Facebook uses these data.

2.7.4 Twitter plugin

Functions of the Twitter service have been integrated into our site. When you use Twitter and the "retweet" function, the websites you visit are connected to your Twitter account and made known to other users. If you are not yet logged into your Twitter account, clicking a Twitter button will show you the Twitter login page for you to enter your login credentials. In doing so, data will also be transferred to Twitter. We would like to point out that we have no knowledge of the content of the data transmitted or how it will be used by Twitter.

2.7.5 Instagram plugin

Our site contains functions of the Instagram service.

If you are logged into your Instagram account, you can click the Instagram button to link the content of our pages with your Instagram profile. This means that Instagram can associate visits to our pages with your user account. If you are not yet logged into your Instagram account, clicking an Instagram button will show you the Instagram login page for you to enter your login credentials. We expressly point out that we receive no information on the content of the transmitted data or its use by Instagram.

2.7.6 YouTube plugins

Our site uses plugins from YouTube, which is operated by Google.

If you visit one of our pages featuring a YouTube plugin, it is a connection to the YouTube servers. Here, the YouTube server is informed about which pages you have visited.



If you're logged in to your YouTube account, YouTube allows you to associate your browsing behavior directly with your personal profile. You can prevent this by logging out of your YouTube account. If you are not yet logged in, clicking a YouTube button will show you the YouTube login page for you to enter your login credentials.

2.7.7 Social Media Tools

LinkedIn Lead Gen Forms

KBL uses LinkedIn Lead Gen Forms for KBL sponsored content, and sponsored LinkedIn InMails for recruitment and marketing campaigns. Once LinkedIn members click on KBL advertisement, they will see a form that is pre-filled with information from their LinkedIn profile, such as their name, contact information, company name, seniority, job title and location. As soon as a LinkedIn member submits a lead form, they will be connected to KBL.

2.7.8 Google Maps

Our site uses the Google Maps map service via an application programming interface (API).

To use Google Maps, it is necessary to save your IP address. This information is generally translated to a Google server in the United States and stored there. We have no influence on this data transfer.

2.7.9 Legal grounds for processing personal data of visitors to our social media pages, and the use of social media plugins and tools are:

- Our legitimate interest in promoting KBL services and brand
- Our legitimate interest in attracting, identifying and sourcing talent
- Our legitimate interest to improve your website experience and to optimize our services

2.8.0 Individuals who correspond with KBL via email

KBL uses a variety of tools to maintain the security of our IT infrastructure, including our email facilities. Examples of such tools are:

- Systems that scan incoming emails to KBL recipients for suspicious attachments and URLs, in order to prevent malware attacks
- Tools that provide end-point threat detection to detect malicious attacks
- Tools that block certain content or websites

If you correspond via email with any KBL recipient, your emails will be scanned by the tools KBL operates to maintain the security of the IT infrastructure, which could result in content being read by authorized KBL persons other than the intended recipient.



2.8.1 Legal grounds for processing personal data of individuals who correspond with KBL via email:

- Our legitimate interest in protecting our IT infrastructure against unauthorized access or data leakage
- Our legitimate interest in analyzing email traffic

2.9.0 Job applicants

We collect information from and about candidates in connection with available employment opportunities at KBL. The information that we collect, the manner in which it is used, and the timing in which it is gathered varies depending on where you are applying from. As general matter, the data we collect regarding our job applicants includes resumes or CVs, identification documents, academic records, work history, employment information and references.

We use your personal data to match your skills, experience and education with specific roles offered by KBL. This information is passed to the relevant hiring officers and persons involved in the recruitment process to decide whether to invite you for an interview. KBL will collect further information if you are invited to the interview (or equivalent) stage and onward. Such information includes interview notes, assessment results, feedback and offer details.

In connection with our recruitment activities including applications and onboarding, we also collect special category data from candidates where we have an employment law obligation to do so. This information is relevant to their future working environment at KBL or the future provision of employment benefits, or with the individual's explicit consent, where collecting such information is permitted by law. For example, where allowed under applicable law, we will collect information about an individual's disabilities in order to analyze the diversity of our workforce.

Once onboarded, an individual's provision of information regarding disabilities will also be used to provide a suitable working environment. We will also need to conduct criminal background checks for certain candidates to assess their eligibility to work at KBL or for KBL customers. In certain countries, we will also ask candidates to provide diversity information about their race and ethnicity, and sexual orientation for diversity monitoring purposes, although the provision of this information will be entirely voluntary. However, where a candidate does not voluntarily provide such information, we could be required by law to make our own assessment of such criteria.

Depending on where you are applying from, KBL collects personal data about candidates ("you") from the following sources:

- Directly from you – for example, information that you have provided when applying for a position directly through the KBL careers website (for additional information about the processing of your personal data.



- From recruitment agencies – for example, when a recruitment agency with your details contacts us to suggest you as a potential candidate
- Through publicly available sources online – for example, where you have a professional profile posted online (e.g., on your current employer's website or on a professional networking site, such as LinkedIn)
- By reference – for example, through a reference from a current or former employee or employer, or from a referee you have identified
- Results of background screening checks

2.9.1 Legal grounds for processing personal data of our job applicants are:

- Explicit consent of the candidate
- Our legitimate interest in attracting, identifying and sourcing talent
- Our legitimate interest to process and manage applications for roles at KBL, including the screening and selecting of candidates
- Our legitimate interest to hire and onboard candidates by making an offer to successful candidates, and carrying out pre-employment screening checks
- Our legitimate interest to manage our career websites (including conducting statistical analyses)
- Compliance with a legal or regulatory obligation (when carrying out background checks to warrant a candidate is eligible to work)

2.10. Alumni

KBL hopes to maintain a lifelong, mutually beneficial relationship with KBL alumni (former employees). If we invite you to our alumni community, your name, contact details, role, last KBL office, rank, service line will be used to create a record for you in one of our databases, unless you have indicated that you are not interested in participating in the KBL alumni program. You have the opportunity to create a more detailed profile and to decide how much additional information you wish to share with KBL and the wider alumni community.

Our alumni databases contain their own privacy notices explaining why and how personal data is collected and processed by those applications. We encourage individuals using our alumni databases to refer to the privacy notices available on those applications.

2.10.1 The legal grounds for processing personal data of our alumni are:

- Explicit consent of the alumnus
- Our legitimate interest in maintaining a strong relationship with our alumni, sending publications about KBL and our services, inviting alumni to events, and helping alumni keeping in touch with other alumni



2.11. Vendors/Suppliers

We process personal data about our Vendors/suppliers (including subcontractors, and individuals associated with our suppliers and contractors) in order to manage our relationship and contract, and to receive services from our suppliers.

The personal data we process is generally limited to contact information (name, name of employer, phone, email and other contact details) and financial information (payment-related information).

In addition, we also use data about our suppliers to check whether we have a conflict of interest to appointing a supplier. Before we take on a new supplier, we also carry out background checks required by law or regulation, for example, adverse media, bribery and corruption, and other financial crime checks.

2.11.1 Legal grounds for processing personal data of our vendors/suppliers are:

- Performance of a contract
- Compliance with a legal or regulatory obligation
- Our legitimate interest in managing payments, fees and charges, and to collect and recover money owed to KBL
- Our legitimate interest in understanding any conflict of interest or challenge with regard to independence legislation
- Our legitimate interest in safeguarding against KBL inadvertently dealing with the proceeds of criminal activities or assist in any other unlawful or fraudulent activities (for example, terrorism)

2.12. KBL/Ethic

KBL/Ethic provides KBL people, customers and others outside of KBL with a means to confidentially, and either anonymously or on a disclosed basis, report an activity that involves unethical or illegal behavior that is in violation of professional standards or otherwise inconsistent with our KBL Code of Business and Ethical Conduct. Reports can be made either online or via a telephone hotline.

KBL/Ethics contains its own privacy notice and consent form which describes the practices KBL follows in relation to KBL/Ethics. We encourage individuals using KBL/Ethics to refer to this KBL/Ethics notice and consent form.

2.13 Vistors to KBL Offices

When you visit KBL Head office and Branches, we process your personal data in order to provide you with certain facilities (such as access to our buildings and conference rooms or Wi-Fi), to control access to our buildings, and to protect our offices, personnel, goods and confidential information (for example, by using CCTV).



The personal data we collect is generally limited to your name, contact information, location, and the time you enter and leave our office.

2.13.1 Visitor records and access badges

We require visitors to our Head office/branches to sign in at reception and we keep that record of visitors for a short period of time. Visitors to our offices are provided with a temporary access badge to access our offices. Our visitor records will be used to verify that access badges are returned, to look into a security incident and for emergency purposes (for example, if an office needs to be evacuated).

2.13.2 Wi-Fi

We monitor and log traffic on our Wi-Fi networks. This allows us to see limited information about a user's network behavior, but will also include being able to see at least the source and destination addresses the user is connecting from and to.

2.13.3 CCTV

KBL uses CCTV monitoring where permitted by law. CCTV images are securely stored and only accessible on a need-to-know basis (for example, to look into an incident). We are allowed to disclose CCTV images to law enforcement bodies. We will also share CCTV images with our insurers for purposes of processing an insurance claim as a result of an incident.

2.13.4 Legal grounds for processing personal data of visitors to KBL offices are:

- Our legitimate interest in protecting our offices, personnel, goods and confidential information
- Our legitimate interest in preventing and detecting crime, and establishing, exercising and defending legal claims

2.14.0 Transfer of personal Data

Certain aspects of the KBL infrastructure are centralized, including information technology services provided to subsidiaries. In addition, where engagements with KBL customers span more than one jurisdiction, certain information will need to be accessed by all those within the KBL organization who are working on the matter.

Therefore, your personal data will be transferred to and stored outside the country in which you are located. This includes countries with laws that have not necessarily been determined to provide an adequate level of protection for the processing of personal data.

We take appropriate security and legal precautions to safeguard the safety and integrity of personal data that is transferred within the KBL organization.

Your personal data will also be processed by KBL support providers that support our internal ancillary processes.



2.15.0 Support Providers

We transfer or disclose the personal data we collect to external support providers (and their subsidiaries and affiliates) who are engaged by us to support our internal ancillary processes. For example, we engage support providers to provide (a) general office support including printing, document production and management, archiving services; (b) accounting, finance and billing support; (c) IT functions including system management and security, data storage, business applications, and replication of systems for business continuity/disaster recovery purposes; and (d) conflict checking, risk management and quality reviews.

It is our policy to only use third-party support providers that are bound to maintain appropriate levels of data protection, security and confidentiality, and that comply with any applicable legal requirements for transferring personal data outside the jurisdiction in which it was originally collected. For data collected in the European Economic Area (EEA) or which relates to data subjects in the EEA, KBL requires an appropriate transfer mechanism as necessary to comply with applicable law.

2.16.0 Other disclosure

KBL discloses your personal data:

- Where this is appropriate for the purposes described in the section “Purposes for which we process personal data,” including within the KBL organization itself
- If required, by applicable law
- In connection with a reorganization or combination of our organization with another organization
- If we believe that such disclosure is appropriate to enforce or apply terms of engagement, and other agreements or otherwise protect and defend KBL rights, property or safety
- In order to comply with a judicial proceeding, court order or other legal obligation, or a regulatory or government inquiry; or
- With your consent

We would like to draw particular attention to the fact that in certain jurisdictions, KBL has a legal obligation to report suspicious transactions and other activity to relevant regulatory authorities under anti-money laundering, terrorist financing, insider dealing or related legislation. KBL also reports suspected criminal activity to the police and other law enforcement bodies. We are not always permitted by the law to inform you about this in advance of the disclosure, or at all.

Third-party recipients of personal data include:

- Professional advisors, such as law firms, tax advisors or auditors
- Insurers
- Audit regulators
- Tax and customs, and excise authorities



- Regulatory and other professional bodies
- Stock exchange and listing authorities
- Public registries of company directors and shareholdings
- Providers of identity verification services
- Credit reference agencies
- The courts, police and law enforcement agencies
- Government departments and agencies
- Service providers
- Support providers

2.17.0 Security

KBL protects the confidentiality and security of information it obtains in the ordinary course of its business. Access to such information is limited, and policies and procedures are in place that are designed to safeguard the information from loss, misuse and improper disclosure.

2.18.0 Keeping your persona data up-to-date

We maintain the accuracy and completeness of the personal data we hold. It is important that you inform us of any updates to your contact details or other personal data so that we have the most up-to-date information about you. Please contact the person you usually deal with at KBL. You can also contact our data protection team.

2.19.0 Retention

Our policy is to retain personal data only for as long as it is needed for the purposes described in the section "Purposes for which we process personal data." However, records of customer information shall be kept for at least 5 years after the closure of the account. The records for financial transactions shall be kept for at least 5 years from the date of the transaction.

2.20.0 Minors

Our Site is not intended for use by minors under the age of eighteen (18) years. KBL does not knowingly collect, disclose, or sell the personal data of minors under 16 years of age. If you are under 18 years old, please do not provide any personal data even if prompted to do so. If you believe that you have inadvertently provided personal data, please ask your parent(s) or legal guardian(s) to notify us and we will delete your personal data.

2.21.0 Amendment of the policy

This policy shall be reviewed and updated every three years. However, where significant developments require amendment of the policy, the review date may be shortened.