BAL GLOBAL FINANCE (UK) LIMITED
BANK OF AMERICA MERRILL LYNCH EUROPE DESIGNATED ACTIVITY COMPANY - LONDON BRANCH
BANK OF AMERICA, N.A. - LONDON BRANCH
MERRILL LYNCH INTERNATIONAL (1) (OC 3322)
ML INVEST HOLDINGS

RECRUITMENT DATA PROTECTION NOTICE

I. INTRODUCTION

One or more of the entities set out above (being the legal entity/ies to which the applicant is applying) (the "Company") has prepared this Recruitment Data Protection Notice ("Notice") to outline their practices regarding the collection, use, storage, transfer and other processing of individually identifiable information collected from or about Applicants ("Personal Data"). For the purposes of this Notice, "Applicant" means any individual who submits Personal Data or about whom Personal Data has been acquired in order to be considered for an actual or potential job vacancy or who attends or applies to attend a career event.

In the event this Notice is provided to an Applicant in a language other than English, any discrepancy, conflict or inconsistency between the two language versions shall be resolved in favour of the English version (subject to applicable law).

II. PERSONAL DATA COLLECTION AND PURPOSES OF USE

Good recruitment and talent management practices and the effective running of our business require the Company to collect, use, store, transfer and otherwise process certain Personal Data.

The Company collects Personal Data that is directly relevant to its business, required to meet its legal obligations, or otherwise permissible to collect under applicable laws. Listed in Appendix A of this Notice are the categories of Personal Data that we collect and the purposes for which we use the data that we collect except where restricted by applicable law. We receive Personal Data from you and from other sources, such as referees, background check providers and public sources.

We collect and process Personal Data about you: (i) because we are required or permitted to do so by applicable law, (ii) because such information is necessary for the performance of your future contract of employment if successful at recruitment stage or in order to take steps at your request prior to entering into that contract, (iii) because such information is of particular importance to us and we have a specific legitimate interest under law to process it (iv) where public interest requires it, (v) where the Personal Data is necessary for the establishment, exercise or defence of legal claims, or (vi) where necessary to protect the vital interests of you or another person.

You are responsible for the content of the information you provide to us and you must ensure it is legal, honest, truthful, accurate and not misleading in any way. You must ensure that the information provided by you does not contain material that is obscene, blasphemous, defamatory, infringing on any rights of any third party, or otherwise legally actionable by such third party. You understand that, in the event that your application is successful, you may be subject to disciplinary action and possible dismissal if the statements contained in the application form and supporting documents prove to be untrue.

The Company does not use the Personal Data of any Applicant for direct or indirect marketing purposes, except where the Company obtains the Applicant's express consent to do so and provides the Applicant with the subsequent right to object at any time and at no charge to the use of Personal Data for direct or indirect marketing purposes.

SENSITIVE PERSONAL DATA

The Company may collect and process certain special or other significant categories of Personal Data ("Sensitive Personal Data") about Applicants where required by applicable law, where necessary for the establishment, exercise or defence of legal claims, or, where necessary, the Applicant has provided explicit consent. Subject to applicable law, the Company may process information about:

- physical and/or mental health for the purposes of addressing potential workplace health, safety and accommodation issues and assessing absence data during the recruitment process
- criminal charges/convictions or unlawful behaviour for recruitment and pre-employment screening purposes and for the assessment of registration and licensing requirements
- sexual orientation, race and/or ethnic origin, gender, gender identity and gender expression, physical and/or mental health for purposes of reporting on diversity and inclusion statistics, complying with government reporting requirements, and/or other legal obligations
- biometric data, such as fingerprints and iris scans, for the purposes of electronic identification, authentication and corporate security, at secured Company premises

PERSONAL DATA ABOUT OTHER INDIVIDUALS

If an Applicant provides the Company with Personal Data about other individuals (e.g., individuals listed by Applicants as referees), it is the Applicant's responsibility to inform such individuals of their rights (see Sections VII and IX) and to obtain their explicit consent, where necessary under applicable law, to the processing (including transfer) of that Personal Data as set out in this Notice.

MEANS OF COLLECTION AND USE

During and in connection with the recruitment and talent identification process and in order to be considered for actual and potential job vacancies, the Company may collect Personal Data directly from Applicants through the completion and submission of online application forms and profiles, through resumes or curricula vitae, or through interviews or other communications (both verbally and in writing) with Applicants. The Company may also collect Personal Data from other sources, including specialist third party providers of recruitment services and publicly available sources. Personal information will be collected to the extent permitted by applicable laws and as appropriate for the actual or potential job vacancy or career event for which the Applicant is seeking to be considered.

Collection, use, processing, disclosure or international transfer of Personal Data may be by automated or manual means, including by hard-copy or soft-copy documents or other appropriate technology.

III. DATA STORAGE AND ACCESS BY COMPANY PERSONNEL

The Company maintains an automated record of the Personal Data of the Applicant. The Company may also maintain hard-copy records on Applicants. The Company maintains these records in a secure environment including in the Company's HR Information System and other applicant tracking systems. Personal Data may be stored in the Applicant's home jurisdiction and/or in other jurisdictions in which the Company has operations.

Where permitted by law, access to Personal Data is restricted to those individuals who need such access for the purposes listed in Appendix A, including but not limited to members of the Human Resources Department and the managers involved in the recruitment process, and to authorised representatives of the Company's internal control functions such as Compliance, Chief Administrative Office, Information Security, Corporate Security, Audit and Legal. Access may also be granted, on a strict need-to-know basis, to others where permitted by law.

IV. DISCLOSURE

Given the global nature of the Company's activities, the Company may (subject to applicable law and for the purposes described in this Notice) transmit Personal Data, including Sensitive Personal Data, to other Bank of America affiliates or operations located in other jurisdictions, including the United States or other jurisdictions where data protection laws may not provide an equivalent level of protection to the laws in the Applicant's home jurisdiction. A list of affiliates belonging to the Bank of America Corporation group is available upon request.

The Company may disclose in accordance with applicable law relevant Personal Data to certain third parties in connection with the provision of services to the Company. Where the processing of Personal Data is delegated to a third party data processor, such as those listed in Appendix A, the Company will delegate such processing in writing, will choose a data processor that provides sufficient guarantees with respect to technical and organisational security measures, such as data protection and information security requirements, governing the relevant processing and will ensure that the processor acts on the Company's behalf and under the Company's instructions.

Personal Data also may be disclosed, where permitted by applicable law, in connection with a corporate restructuring, sale, or assignment of assets, merger, divestiture, or other changes of the financial status of the Company or any of its subsidiary or affiliated Companies. Personal Data also may be released to protect the legitimate interests of the Company (unless this would prejudice the rights and freedoms or interests of the Applicant), or in the Company's judgement to comply with applicable legal or regulatory obligations and regulatory inquiries or requests.

V. INTERNATIONAL TRANSFERS OF PERSONAL DATA AND SENSITIVE PERSONAL DATA

Given the global nature of the Company's activities, the Company may transfer Personal Data, including Sensitive Personal Data, outside an Applicant's home jurisdiction. For Applicants in the European Economic Area ("EEA"), this may include transfers to countries located outside of the EEA. Some of these countries are recognized by the European Commission as providing an adequate level of protection according to EEA standards (the full list of these countries is available here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm). With regard to transfers from the EEA to other countries, we have put in place adequate measures, such as standard contractual clauses adopted by the European Commission to protect your information. Applicants in the EEA may obtain a copy of these measures by following this link: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

VI. SECURITY

The Company maintains appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage to Personal Data.

VII. ACCESS, PORTABILITY AND ACCURACY OF PERSONAL DATA

Applicants are entitled to access Personal Data held about them (with the exception of any documents that are subject to legal privilege, that provide Personal Data about other unrelated individuals, or that otherwise are not subject to data subject access rights). Any Applicant who wishes to access his/her Personal Data or (where permitted under applicable law) request portability of their data should contact a member of the Global Talent Acquisition group using the contact information set out in Section X below.

To the extent required by applicable law, Applicants have the right to have inaccurate data corrected or removed (at no charge to the Applicant and at any time).

To assist the Company in maintaining accurate Personal Data, Applicants must ensure they keep their Personal Data up to date on the Company's online recruitment system or by informing the Global Talent Acquisition group via: internationaltalentacquisitionoperations@bankofamerica.com. In the event that the Company becomes aware of any inaccuracy in the Personal Data it has recorded, it will correct that inaccuracy at the earliest practical opportunity.

VIII. MODALITIES OF THE PROCESSING AND DATA RETENTION

The processing of Personal Data is carried out with the aid of manual and electronic tools.

The Company will maintain your Personal Data for as long as it is required to do so by applicable law(s) or for as long as necessary for the purpose(s) of use and processing in Section II, whichever is longer ("Initial Retention Period"). With the exception of the countries listed below, if your application is unsuccessful your Personal Data will be retained for an Initial Retention Period of 6 months.

In addition the Company will, with your consent, retain your Personal Data after the expiry of the Initial Retention Period in its talent management database so that it may contact you with details of suitable positions that arise and which may be of interest to you. If you do not wish the Company to retain your Personal Data in its talent management database after the expiry of the Initial Retention Period you may request that your Personal Data be deleted. You may make this request at any time, but your request will not be actioned until the Initial Retention Period has expired. With the exception of the countries listed below, if your application is unsuccessful, unless you do not consent to your Personal Data being retained by the Company in its talent management database or you subsequently request that your Personal Data be deleted, your Personal Data will be retained for a total of 2 years after the date of last recorded contact with you.

Any maximum storage term set forth by applicable law will prevail. The Company will delete Personal Data after the applicable retention period.

Country	**Period of retention**
Germany	6 months
Netherlands	1 year

For the United Kingdom, the Company may be obliged to keep Personal Data of unsuccessful candidates considered for a position impacted by the Resident Labour Market Test where the selected candidate is a sponsored immigrant, in which case the Personal Data will be retained for 7 years.

If your application is successful, your application is retained as part of your personnel record.

IX. OTHER RIGHTS AND CONSEQUENCES

To ensure good recruitment and talent management practices and the effective running of the Company's business, it is mandatory for the Company to collect, use, store, transfer and otherwise process the Personal Data marked with an asterisk in Appendix A (unless otherwise indicated during the application process). It is voluntary for Applicants to provide other types of Personal Data and information about themselves.

To the extent available under applicable law, Applicants have the right to object to the collection, use, storage, transfer or other processing of Personal Data as described in this Notice, the right to withdraw consent to or request discontinuance of collection, use, storage, transfer or other processing of Personal Data as described in this Notice, and to request deletion of such Personal Data. However, objections to the collection, use, storage, transfer or other processing of Personal Data, withdrawals of consent, requests for discontinuance and requests for deletion may affect the Company's ability to consider an Applicant for an actual or potential job vacancy or career event and to process a related application for employment to the extent that the purposes set out in this Notice cannot be achieved.

Any Applicant who wishes to object to the collection, use, storage, transfer or other processing of Personal Data as described in this Notice, to withdraw consent, to request discontinuance or to request deletion should contact a member of the Global Talent Acquisition group using the contact information set out in Section X below.

Under applicable law, in certain circumstances, the Company may be exempt from or entitled to refuse the above requests or rights. Certain additional terms and conditions may be applicable to process requests or rights, such as requiring communications to be in writing or requiring proof of identity.

X. QUESTIONS

Should any Applicant have any questions, concerns or complaints about this Notice, please contact a member of the Global Talent Acquisition group via: internationaltalentacquisitionoperations@bankofamerica.com

The Company will make every effort to resolve any questions, concerns or complaints promptly and in accordance with applicable law.

If you have additional queries about the way in which the Company processes your Personal Data please contact the EU Data Protection Officer using the following contact details: bofa.eudpo@bofa.com

You may have the right to lodge a complaint with the Data Protection Authority for your country.

XI. CHANGES TO THIS NOTICE

The most up-to-date Notice is posted to the Bank of America Careers Website.

Appendix A

The Categories of Personal Data We May Collect, Use, Transfer And Disclose:

- **Recruitment/Applicant information:** Employment history*; Employer name*; language(s) spoken*; previous compensation*; Pre-employment references, voice and video recording
- **Media Checks:** Publicly available information
- **Employment and Job Information:** Job title and/or position and description of responsibilities/duties*; location; band/seniority; department; line and sub-line of business; local Bank entity name; employment dates; supervisor/manager/team lead name and contact information
- **Personal Demographic Information:** Gender; date and place of birth; name (including birth surname and any other former names)*; family/marital status
- **Diversity and Inclusion:** gender, gender identity, gender expression, socio-economic background
- **Visa/ Citizenship Details:** Work eligibility status; entitlement to residency*; nationality, citizenship; passport details; visa details; National ID, social insurance number or other tax identifier number
- **Contact Details:** Address, telephone, email details* and emergency contact details
- **Expenses:** Bank account details
- **Applicant Administration:** Applicant tracking records and query management records*; voice recording and video recording; Reference letters; query management records
- **Absence Data:** Absence details e.g. sickness
- **Attendance Data:** Working Time Directive Details
- **Physical Security and Life Safety Data:** Swipe card entry data; CCTV; photograph (Security ID Card where applicable); accident and incident reporting; Biometrics
- **Compensation:** Compensation information (including base salary, market rates, incentive payment(s), stock options information and allowances)
- **Education and Training:** Academic and educational record*, professional qualifications* and memberships; professional training*
- **Regulatory Data (where applicable):** Licenses and certifications*; financial or other regulatory registration*
- **Technical information:** Including username, passwords and IP addresses.
- **Sensitive Personal Data:** Information regarding physical and/or mental health* (if required to make reasonable adjustments in the Recruitment Process), sexual orientation, race and/or ethnic origin, criminal charges/convictions or unlawful behaviour for recruitment and pre-employment screening purposes and for assessment of registration and licensing requirements, biometric data, such as fingerprints and iris scans, for the purposes of electronic identification, authentication and corporate security, at secured Company premises

* Personal Data marked with an asterisk in this Section is mandatory for Applicants to provide to the Company (unless otherwise indicated during the application process). It is voluntary for Applicants to provide other types of Personal Data and information about themselves. Some of the personal data listed above may be shared, collected, used, transferred and/or disclosed in-line with country specific laws/regulations at offer stage.

The Purposes For Which We May Collect, Use, Transfer And Disclose Personal Data:

- **Recruiting activities, talent management, succession planning, expense management and general administration** e.g. event management materials, keeping your application data on file, communication with Applicants about any actual or potential job vacancy or career event, conduct of interviews, consideration of eligibility for selection as candidate for employment, and offer approval
- **Authentication/identification of Applicants**
- **Human resources information systems ("HRIS") and application support and development**
- **Information technology and information security support** (including anti-spam and virus protection, and cyber security monitoring)
- **Diversity and inclusion data analysis** (anonymized and aggregated)
- **Management of internal business operations** (internal business processes such as data analysis, monitoring, testing and audits)
- **Complying with applicable government reporting and other applicable and foreign law requirements** (including the requirements of the US Sarbanes-Oxley Act or other applicable internal control regulations and in such areas as immigration, tax or statutory financial regulation) and other legal obligations
- **Defending, preparing for, participating in and responding to potential legal claims, investigations and regulatory inquiries** (all as allowed by applicable law)

The Categories Of Unaffiliated Third Parties With Whom We May Share Personal Information:

- **Professional Advisors:** Accountants, auditors, lawyers, and other outside professional advisors in all of the countries in which the Company operates

- **Service Providers:** Companies that provide products and services to the Company in the countries in which the Company operates, such as human resources services and recruitment; expense management, relocation services, IT systems suppliers and support; reception and security, catering and logistics services providers, translation services, third parties assisting with event organising and marketing activities, medical or health practitioners, and other service providers
- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over the Company in the countries in which the Company operates, such as regulatory authorities, law enforcement, public bodies, licensing and registration bodies, judicial bodies and third parties appointed by such authorities
- **Parties Related to a Corporate Transaction:** A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of the Company's business, assets or stock (including in connection with any bankruptcy or similar proceedings), e.g., stock exchanges and business counterparties