Chang Hwa Commercial Bank London Branch
Employee/Worker/Contractor Privacy Statement

This privacy statement sets out what personal data Chang Hwa Commercial Bank London Branch ('the Bank') (under the register number BR000414 with registered address at 4F, 6-8 Tokenhouse Yard, London EC2R 7AS) collects about you, what the personal data is used for, the legal basis which permits us to use it and the safeguards we put in place to protect it. It also sets out your rights and how to lodge a complaint in relation to personal data.

Contact details

We have appointed a Data Protection Officer who has responsibility for advising us on our data protection obligations. You can contact our Data Protection Officer using the details below:

Address:	The Data Protection Officer Chang Hwa Commercial Bank London Branch 4th Floor, 6-8 Tokenhouse Yard, London EC2R 7AS
Tel:	0207 600 6600
Email:	dataprotection@chblondon.com

What is personal data?

Personal data is any information that tells us something about you. This could include information such as your name, contact details, date of birth, medical information and bank account details.

How do we collect personal data?

We collect personal data about you from various sources including:

- from you when you contact us directly through the application and recruitment process or during your employment/engagement;
- from other people when we check references or carry out background checks – if we do this we will inform you during the recruitment process of the exact checks that are carried out;
- any personal data we obtain from searching public records, such as the Electoral Roll, to help us verify your identity; and
- we also collect information about job-related activities through the course of your employment/engagement with us.

What Personal Data we collect

In order to meet the local and EU data protection requirements, the Bank may collect the following personal data from our employees ('individuals' or 'you') whether they are in the UK, European Union or outside the EU, from time to time:

- Personal contact details such as name, title, address, telephone numbers and personal email addresses
- Date of birth
- Place of birth
- Gender

- Marital status and dependents
- Next of kin and emergency contact information
- National insurance number
- Right to work information and documentation including visas
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start and end date of employment/engagement
- Location of employment or workplace
- Copy of your driving licence and motor insurance documentation if we provide you with a company car or if you drive as part of your employment/engagement
- Recruitment information (including copies of right to work documentation, qualifications, references and other information in your CV or cover letter or otherwise provided as part of the application process)
- Copies of identification documents such as your passport and driving licence
- Employment/engagement records (including job titles, work history, working hours, training records and professional memberships)
- Compensation/expenses records
- Performance information (including appraisals)
- Disciplinary and grievance information (whether or not you are the main subject of those proceedings)
- CCTV footage and other information obtained through electronic means such as swipecard records
- Information about your use of our information and communication systems
- Photographs and video footage
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences committed by you

Additionally, we may monitor or record phone calls with customers, staff or suppliers in case we need to check we have carried out customers instruction correctly, to resolve queries or issues, for regulatory purposes, to help improve the Bank's quality of service, and to help detect or prevent frauds.
Conversations may also be monitored for staff training purposes.

For the protection of safety of our customers, visitors and employees, we also operate CCTV in our premises.

Purposes of Data Collection

The Bank may use collected Personal Data for the following purposes:

- To make decisions about your recruitment and appointment
- To determine the terms on which you work/provide services for us
- To check you are legally entitled to work in the UK
- To pay you and, if you are an employee, to deduct tax and national insurance contributions
- To provide benefits to you, including pensions and other benefits
- To liaise with your pension provider
- To administer the contract we have with you
- For business management and planning purposes, including accounting and auditing
- To conduct performance reviews, manage performance and determine performance requirements
- To make decisions about salary reviews and compensation
- To assess your qualifications for a particular job or task, including decisions about promotions
- To decide whether and how to manage your conduct
- To gather evidence for possible grievance or disciplinary hearings (in relation to you or someone else)
- To make decisions about your continued employment or engagement
- To make arrangements for the termination of our working relationship
- For education, training and development
- To deal with legal disputes involving you or other employees, workers or contractors, including accidents at work
- To provide information to regulators (PRA and FCA) for the approved persons and certification purposes
- To ascertain your fitness for work
- To manage sickness absence

- To inform next of kin in case of a personal emergency
- To comply with health and safety obligations
- To prevent and detect fraud or other criminal offences
- To monitor compliance with our policies and our contractual obligations, including the use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- To carry out equal opportunities monitoring
- For insurance purposes
- To provide a reference upon request from another employer/third party
- For PR, marketing and internal communications
- To comply with employment law, immigration law, health and safety law, tax law and other laws which affect us

We do not take automated decisions about you using your personal data or use profiling in relation to you.

What is the legal basis that permits us to use your personal data?

Under data protection legislation we are only permitted to use your personal data if we have a legal basis for doing so as set out in the data protection legislation. We rely on the following legal bases to use your personal data for employment/engagement related purposes:

- Where we need your personal data to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

In more limited circumstances we may also rely on the following legal bases:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

The table at the end of this notice provides more detail about the personal data that we use, the legal basis that we rely on in each case and your rights.

Some personal data is classified as "special" data under data protection legislation. This includes information relating to ethnicity, political opinions, religious beliefs, trade union membership, the processing of genetic data, biometric data, sexuality or health. This personal data is more sensitive and we need to have further justifications for collecting, storing and using this type of personal data. There are also additional restrictions on the circumstances in which we are permitted to collect and use criminal conviction data. We may process special categories of personal data and criminal conviction information in the following circumstances:

- In limited circumstances with your explicit consent, in which case we will explain the purpose for which the personal data will be used at the point where we ask for your consent.

- We will use information about your physical and mental health or disability status to comply with our legal obligations, including to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

- We will use information about criminal offences to comply with our regulatory obligations such as Money Laundering Regulations and Senior Manager and Certification Regime requirements. This may include ongoing monitoring.

What happens if you do not provide the personal data that we request?

We need some of your personal data in order to perform our contract with you. We also need some personal data so that we can comply with our legal obligations.

Where personal data is needed for these purposes if you do not provide it we will not be able to perform our contract with you and may not be able to offer employment/engagement or continue with your employment/engagement. We explain when this is the case at the point where we collect personal data from you.

How do we share your personal data?

We share your personal data in the following ways:

- With our Head Office as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

- Where we use third party services providers who process personal data on our behalf in order to provide services to us. This includes IT systems providers and IT contractors, payroll providers, Human Resources consultants, Criminal Records checking agencies and pension administration providers.

- We will share your personal data with regulators, including Financial Conduct Authority, Prudential Regulation Authority or other government crime agencies, where we are required to do so to comply with our regulatory obligations.

- We will share your personal data with third parties where we are required to do so by law. For example, we are required to provide tax-related information to HMRC.

- If we sell any part of our business and/or integrate it with another organisation your details may be disclosed to our advisers and to prospective purchasers or joint venture partners and their advisers. If this occurs the new owners of the business will only be permitted to use your personal data in the same or similar way as set out in this privacy notice.

Where we share your personal data with third parties we ensure that we have appropriate measures in place to safeguard your personal data and to ensure that it is solely used for legitimate purposes in line with this privacy notice.

Retention Period of Personal Data

As a general rule we keep your personal data for the duration of your employment/engagement and for a period of 7 years after your employment/engagement ends and in relation to job applicants, for a period of 6 months after candidates have been notified that their application for a position was unsuccessful. However, where we have statutory obligations to keep personal data for a longer period or where we may need your personal data for a longer period in case of a legal claim, then the retention period may be longer. Full details of the retention periods that apply to your personal data are set out in our Data Retention Policy which is available by writing to dataprotection@chblondon.com.

Data will be deleted from our systems in accordance with the law and our technical capabilities.

Safeguarding of Personal Data and Transfer Overseas

The security of personal data is crucial to us. When personal data is transferred to countries outside of the UK and the European Economic Area those countries may not offer an equivalent level of protection for personal data to the laws in the UK. Where this is the case we will ensure that appropriate safeguards are put in place to protect your personal data.

The countries to which your personal data is transferred and the safeguards in place are detailed below:

Taiwan (Head Office)	Data is transferred as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data and for Head Office's approval on employment, promotion, training, pay and reward, benefits matters.	We rely on the European Commission standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.

If you would like to see a copy of the adequacy mechanisms that we use to protect your personal data please contact our Data Protection Officer (please see the contact details above).

We comply with our Information System Security Policy and Procedures which set out security standards. We require the same level of security from our third- party service providers and Head Office in Taiwan.

We do not share your personal data with marketing companies. The use of personal data will be kept to the minimum and strictly for the purposes listed above. Personal data will be held securely and treated confidentially by the Bank.

Your Rights

You have a number of rights in relation to your personal data, these include the right to:

- be informed about how we use your personal data;
- obtain access to your personal data that we hold;
- request that your personal data is corrected if you believe it is incorrect, incomplete or inaccurate;
- request that we erase your personal data in the following circumstances:
    - if we are continuing to process personal data beyond the period when it is necessary to do so for the purpose for which it was originally collected;
    - if we are relying on consent as the legal basis for processing and you withdraw consent;
    - if we are relying on legitimate interest as the legal basis for processing and you object to this processing and there is no overriding compelling ground which enables us to continue with the processing;
    - if the personal data has been processed unlawfully (i.e. in breach of the requirements of the data protection legislation);
    - if it is necessary to delete the personal data to comply with a legal obligation;
- ask us to restrict our data processing activities where you consider that:
    - personal data is inaccurate;
    - our processing of your personal data is unlawful ;
    - where we no longer need the personal data but you require us to keep it to enable you to establish, exercise or defend a legal claim;
    - where you have raised an objection to our use of your personal data;
- request a copy of certain personal data that you have provided to us in a commonly used electronic format. This right relates to personal data that you have provided to us that we need in order to perform our agreement with you and personal data where we are relying on consent to process your personal data;
- object to our processing of your personal data where we are relying on legitimate interests or exercise of a public interest task to make the processing lawful. If you raise an objection we will carry out an assessment to determine whether we have an overriding legitimate ground which entitles us to continue to process your personal data;

- not be subject to automated decisions which produce legal effects or which could have a similarly significant effect on you.

If you would like to exercise any of your rights or find out more, please contact our Data Protection Officer.

The table at the end of this notice provides more detail about the personal data that we use, the legal basis that we rely on in each case and your rights.

Lodging a Complaint

If you wish to raise a complaint regarding the processing of your personal data or are unsatisfied with how we have handled your information, you may contact us at dataprotection@chblondon.com, call us 0207 600 6600 or write to us at the above address. You also have the right to lodge a complaint with the supervisory authority the Information Commissioner's Officer (*tel: 03031231113*) or visit their website https://ico.org.uk/concerns/.

The Bank may update this Privacy Statement from time to time. If we make material changes to the statement, we will notify you of these changes. This Privacy statement was updated in October 2018.

Table: quick check of how we use your personal data

Purpose	Personal data used	Legal basis	Which rights apply?*
Recruitment decisions	Personal contact information, national insurance number, recruitment information including qualifications, references and other information in your CV or cover letter or otherwise provided as part of the application process, employment/ engagement records, compensation history, identification documents such as your passport or driving licence.	Legitimate interest. It is in our interests to ensure we recruit the best possible candidates in order to achieve our business goals and objectives.	The generally applicable rights plus the right to object.
Right to work checks	Information relating to your right to work status, national insurance number, passport number, nationality, tax status information, and personal contact details.	Legitimate interest. It is in our interests to ensure that those who work for us have the right to work in the UK as well as to establish the statutory excuse to avoid liability for the civil penalty for employing someone without the right to undertake the work for which they are employed.	The generally applicable rights plus the right to object.
Performance reviews and appraisals, salary reviews and promotion decisions	Employment/ engagement records, salary and compensation history, performance history, disciplinary and grievance information.	Contractual necessity and legitimate interest. It is in our interests as well as the interests of our employees/ workers/ contractors to have performance and salary/ fee reviews to ensure employees/ workers/ contractors are being adequately compensated	The generally applicable rights plus the right to data portability and the right to object.

		which will in turn motivate them to deliver a high standard of work, ultimately having a positive impact on achieving our business goals.	
Administration of your contract and benefits, including payment of salary/fee and expenses	Compensation history, national insurance number, personal contact information, bank account details, payroll records and tax status information, start and end date of employment/ engagement, date of birth, marital status and dependents, annual leave information, benefits information, pensions information, location of employment or workplace.	Contractual necessity and legitimate interests. It is in our interests as well as the interests of our employees/ workers/ contractors to ensure that the contract is administered properly.	The generally applicable rights plus the right to data portability and the right to object.
Administration of pension schemes	Compensation history, national insurance number, personal contact information, bank account details, payroll records and tax status information, start and end date of employment/ engagement, date of birth and contribution entitlements.	Legal obligation, contractual necessity and legitimate interest. It is in our interests to adequately incentivise our employees to motivate them to deliver a high standard of work, ultimately having a positive impact on achieving our business goals. It is in the interests of the trustees/ scheme administrator to be able to effectively run the pension scheme.	The generally applicable rights plus the right to data portability and the right to object.
Compliance with our statutory duties to ensure a safe place	Information about your health, including any medical condition, health and sickness records and	Legal obligation.	The generally applicable rights only.

of work and to ensure that you are fit for work	location of employment or workplace.		
Management of sickness absence	Personal contact details, employment/ engagement records (sickness hours/days) and information about your health.	Legal obligation and contractual necessity.	The generally applicable rights plus the right to data portability.
To monitor compliance with our policies	Personal contact details, information about your use of our information and communication systems, CCTV footage and other information obtained through electronic means such as swipecard records, disciplinary and grievance information and performance information.	Legitimate interest. It is in our interests to ensure employees/ workers/ contractors are complying with our policies as non-compliance with policies can result in termination of employment/ engagement, ultimately affecting our day to day operations and business plans.	The generally applicable rights plus the right to object.
Fraud and crime prevention	Information about criminal convictions and offences committed by you, personal contact details and CCTV footage and other information obtained through electronic means such as swipecard records.	Public interest and legitimate interest. It is in our interests as well as the interests of our employees/ workers/ contractors to ensure the prevention of fraud and crime is monitored. This will ensure a safe workplace for all.	The generally applicable rights plus the right to object.
Disciplinary and grievance procedures	Personal contact details, disciplinary and grievance information and performance information.	Legitimate interests. It is in our legitimate interests to manage the performance of employees and ensure that disciplinary action is taken where appropriate.	The generally applicable rights plus the right to object.

To deal with legal disputes	Personal contact details, employment/ engagement records, compensation history, performance information, disciplinary and grievance information, photographs and video footage, CCTV footage and other information obtained through electronic means and information about criminal convictions and offences committed by you.	Legitimate interest. It is in our interests to process personal data to make and defend legal claims to ensure that our legal rights are protected.	The generally applicable rights plus the right to object.
Business management and business planning	Information about your use of our information and communication systems, employment/ engagement records, location of workplace, salary, benefit and pension information, personal contact details, photographs.	Legitimate interests. It is in our interests to undertake this processing to ensure we can improve any business operations which will ultimately improve the overall quality of work/ the workplace. Employees/ workers/ contractors will ultimately benefit as the workplace and its procedures may be strengthened.	The generally applicable rights plus the right to object.
Exit management at the end of your employment/engagement	Personal contact details, payroll records, tax status information, end date of employment/ engagement, and employment/ engagement records.	Legitimate interest. It is in our interests as well as the interests of our employees/ workers/ contractors to undertake exit management steps to ensure the employees/ workers/ contractors can express any feedback to us which we can consider and decide whether to implement to improve	The generally applicable rights plus the right to object.

		the workplace for other employees/ workers/ contractors.	
Submit records and register directors at Companies House	Personal contact details including former forenames or surnames (if any), date of birth, nationality, occupation, country of residence.	Legal obligation.	The generally applicable rights.
Emergency contact	Next of kin and emergency contact information	Legitimate interest. It is our interests as well as the interests of our employees/ workers/ contractors for us to hold details of who to contact in an emergency situation.	The generally applicable rights plus the right to object.
PR, marketing and internal communications	Name, job title, career history, photographs and video footage	Legitimate interest. It is in our interests to publicise our services to clients/ customers and third parties. It is in our interests as well those who work for us or on our behalf, or who are on placement with us, to keep them informed of our business and other activities.	The generally applicable rights plus the right to object.
Compliance with regulatory duties	Name, job title, job role, career history, criminal record checks, ID information, contact information, references, CV, qualifications, residential address.	Legal Obligation. Senior Management and Certification Regime as required by the FCA and PRA on Approved Persons and Certification regime. Money Laundering regulations requirement of screening of relevant employees and agents appointed by the firm.	The generally applicable rights only.

*The following generally applicable rights always apply: right to be informed, right of access, right to rectification, right to erasure, right to restriction and rights in relation to automated decision making. For more detail about your rights and how to exercise them please see Your rights in relation to your personal data.